Weiterbildender Masterstudiengang

Secure Information Management

tech technologische universität

tech technologische universität

Weiterbildender Masterstudiengang

Secure Information Management

- Modalität: **online**
- Dauer: **2 Jahre**
- Qualifizierung: **TECH Technologische Universität**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: www.techtitute.com/de/informatik/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-secure-information-management

Index

01 Präsentation des Programms — Seite 4

02 Warum an der TECH studieren? — Seite 8

03 Lehrplan — Seite 12

04 Lehrziele — Seite 32

05 Karrieremöglichkeiten — Seite 38

06 Studienmethodik — Seite 42

07 Lehrkörper — Seite 52

08 Qualifizierung — Seite 62

01

Präsentation des Programms

Im heutigen digitalen Zeitalter werden Aktivitäten in einer Vielzahl von Bereichen vollständig über das Internet abgewickelt. Unterhaltung, Arbeit und Kommunikation mit Freunden und Familie hängen zunehmend von Online-Tools und -Ressourcen ab. Täglich werden enorme Informationsmengen übertragen, von einfachen Daten in Social-Media-Konversationen und Messaging-Anwendungen bis hin zu sensiblen persönlichen und beruflichen Informationen, die auf Bank- oder Unternehmensplattformen gehostet werden. Dieses Szenario erfordert Spezialisten, die in der Lage sind, Informationen in verschiedenen Kontexten zu handhaben und zu schützen, wobei deren Sicherheit Vorrang hat. Aus diesem Grund hat TECH diesen Studiengang in Software Engineering entwickelt, der darauf abzielt, Fachleute mit den notwendigen Fähigkeiten auszustatten, um Informationen effektiv zu verwalten und zu schützen, die aktuellen digitalen Herausforderungen zu bewältigen und dazu beizutragen, sicherere und zuverlässigere technologische Umgebungen zu schaffen.

Der Schutz von Daten ist angesichts der ständigen Bedrohungen von entscheidender Bedeutung. Sie könnten der Hüter dieser wertvollen Informationen sein“

Jede Sekunde werden Tausende von Daten in der digitalen Umgebung erzeugt, ausgetauscht und gespeichert. Von Online-Zahlungen über den Zugang zu Bildungsdiensten bis hin zur Koordinierung von Geschäftsaktivitäten und dem Schutz digitaler Identitäten - die Technologie ist zu einem wesentlichen Pfeiler geworden, der die Art und Weise, wie wir leben und arbeiten, kontinuierlich verändert. Bei diesen Interaktionen werden in jedem Moment riesige Datenmengen erzeugt und übertragen, von persönlichen Informationen bis hin zu sensiblen Dateien von Unternehmen und Institutionen. Dieser ständige Datenfluss macht deutlich, wie wichtig ein angemessener Umgang mit diesen Daten ist, um ihre Sicherheit und ihren Schutz zu gewährleisten.

Die Verwaltung und der Schutz dieser Daten ist keine einfache Aufgabe, da sie eine Kombination aus hochspezialisiertem Fachwissen in Bereichen wie Cybersicherheit und Informationsmanagement erfordert. Diese Disziplinen sind zwar unterschiedlich, müssen aber integriert werden, um die komplexen Herausforderungen des heutigen digitalen Umfelds zu bewältigen. In diesem Zusammenhang stellt der Weiterbildende Masterstudiengang in Secure Information Management eine einzigartige Gelegenheit für Ingenieure und IT-Fachleute dar, die daran interessiert sind, eine umfassende Vision zu erwerben, die sie in die Lage versetzt, beide Bereiche zu beherrschen und sich in einem ständig wachsenden Sektor als Führungskraft zu positionieren.

Viele Unternehmen und Institutionen sehen sich mit der Notwendigkeit konfrontiert, kritische und hochsensible Daten zu schützen, aber es fehlt ihnen an Experten, die eine effiziente Verwaltung, Bewahrung und Überwachung ihrer digitalen Informationen gewährleisten können. Um dieser Nachfrage gerecht zu werden, hat TECH ein Programm entwickelt, das die besten Inhalte mit einem Dozententeam aus renommierten Fachleuten kombiniert. Auf diese Weise wird sichergestellt, dass die Studenten die erforderlichen Instrumente und Kenntnisse erwerben, um sich auf dem Arbeitsmarkt zu behaupten und Zugang zu strategischen Positionen in Unternehmen zu erhalten, die ihre Informationssicherheit stärken wollen.

Dieser **Weiterbildender Masterstudiengang in Secure Information Management** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für Secure Information Management vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren wissenschaftlichen und praktischen Informationen
- Praktische Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens genutzt werden kann
- Mit besonderem Schwerpunkt auf innovativen Methoden für das Secure Informaction Management
- Theoretische Lektionen, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugangs zu Inhalten von jedem festen oder tragbaren Gerät mit Internetanschluss

Erwerben Sie die notwendigen Fähigkeiten, um Daten in einem wettbewerbsorientierten digitalen Umfeld zu sichern und effektiv zu verwalten“

Vertiefen Sie Ihr theoretisches Wissen mit den zahlreichen praktischen Ressourcen, die in diesem Weiterbildenden Masterstudiengang in Secure Information Management enthalten sind“

Entdecken Sie die innovativste Lehrmethode, die von TECH entwickelt wurde, um ein intensives und kontextbezogenes Lernen zu gewährleisten.

Sie haben Zugang zu einem 100%igen Online-Programm, das es Ihnen ermöglicht, jederzeit und von jedem Ort der Welt aus in Ihrem eigenen Tempo zu lernen.

Zu den Dozenten gehören Fachleute aus dem Bereich Finanzen, die ihre Erfahrungen in dieses Programm einbringen, sowie anerkannte Spezialisten aus führenden Gesellschaften und renommierten Universitäten.

Die multimedialen Inhalte, die mit den neuesten Bildungstechnologien entwickelt wurden, ermöglichen der Fachkraft ein situiertes und kontextbezogenes Lernen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem der Student versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Dabei wird die Fachkraft durch ein innovatives interaktives Videosystem unterstützt, das von anerkannten Experten entwickelt wurde.

02

Warum an der TECH studieren?

TECH ist die größte digitale Universität der Welt. Mit einem beeindruckenden Katalog von über 14.000 Hochschulprogrammen, die in 11 Sprachen angeboten werden, ist sie mit einer Vermittlungsquote von 99% führend im Bereich der Beschäftigungsfähigkeit. Darüber hinaus verfügt sie über einen beeindruckenden Lehrkörper mit mehr als 6.000 Professoren von höchstem internationalem Prestige.

Studieren Sie an der größten digitalen Universität der Welt und sichern Sie sich Ihren beruflichen Erfolg. Die Zukunft beginnt bei TECH“

Die beste Online-Universität der Welt laut FORBES

Das renommierte, auf Wirtschaft und Finanzen spezialisierte Magazin Forbes hat TECH als „beste Online-Universität der Welt" ausgezeichnet. Dies wurde kürzlich in einem Artikel in der digitalen Ausgabe des Magazins festgestellt, in dem die Erfolgsgeschichte dieser Einrichtung „dank ihres akademischen Angebots, der Auswahl ihrer Lehrkräfte und einer innovativen Lernmethode, die auf die Ausbildung der Fachkräfte der Zukunft abzielt", hervorgehoben wird.

Die besten internationalen Top-Lehrkräfte

Der Lehrkörper der TECH besteht aus mehr als 6.000 Professoren von höchstem internationalen Ansehen. Professoren, Forscher und Führungskräfte multinationaler Unternehmen, darunter Isaiah Covington, Leistungstrainer der Boston Celtics, Magda Romanska, leitende Forscherin am Harvard MetaLAB, Ignacio Wistumba, Vorsitzender der Abteilung für translationale Molekularpathologie am MD Anderson Cancer Center, und D.W. Pine, Kreativdirektor des TIME Magazine, um nur einige zu nennen.

Die größte digitale Universität der Welt

TECH ist die weltweit größte digitale Universität. Wir sind die größte Bildungseinrichtung mit dem besten und umfangreichsten digitalen Bildungskatalog, der zu 100% online ist und die meisten Wissensgebiete abdeckt. Wir bieten weltweit die größte Anzahl eigener Abschlüsse sowie offizieller Grund- und Aufbaustudiengänge an. Insgesamt sind wir mit mehr als 14.000 Hochschulabschlüssen in zehn verschiedenen Sprachen die größte Bildungseinrichtung der Welt.

Die umfassendsten Lehrpläne in der Universitätslandschaft

TECH bietet die vollständigsten Lehrpläne in der Universitätslandschaft an, mit Lehrplänen, die grundlegende Konzepte und gleichzeitig die wichtigsten wissenschaftlichen Fortschritte in ihren spezifischen wissenschaftlichen Bereichen abdecken. Darüber hinaus werden diese Programme ständig aktualisiert, um den Studenten die akademische Avantgarde und die gefragtesten beruflichen Kompetenzen zu garantieren. Auf diese Weise verschaffen die Abschlüsse der Universität ihren Absolventen einen bedeutenden Vorteil, um ihre Karriere erfolgreich voranzutreiben.

Eine einzigartige Lernmethode

TECH ist die erste Universität, die *Relearning* in allen ihren Studiengängen einsetzt. Es handelt sich um die beste Online-Lernmethodik, die mit internationalen Qualitätszertifikaten renommierter Bildungseinrichtungen ausgezeichnet wurde. Darüber hinaus wird dieses disruptive akademische Modell durch die „Fallmethode" ergänzt, wodurch eine einzigartige Online-Lehrstrategie entsteht. Es werden auch innovative Lehrmittel eingesetzt, darunter ausführliche Videos, Infografiken und interaktive Zusammenfassungen.

Die offizielle Online-Universität der NBA

TECH ist die offizielle Online-Universität der NBA. Durch eine Vereinbarung mit der größten Basketball-Liga bietet sie ihren Studenten exklusive Universitätsprogramme sowie eine breite Palette von Bildungsressourcen, die sich auf das Geschäft der Liga und andere Bereiche der Sportindustrie konzentrieren. Jedes Programm hat einen einzigartig gestalteten Lehrplan und bietet außergewöhnliche Gastredner: Fachleute mit herausragendem Sporthintergrund, die ihr Fachwissen zu den wichtigsten Themen zur Verfügung stellen.

Führend in Beschäftigungsfähigkeit

TECH ist es gelungen, die führende Universität im Bereich der Beschäftigungsfähigkeit zu werden. 99% der Studenten finden innerhalb eines Jahres nach Abschluss eines Studiengangs der Universität einen Arbeitsplatz in dem von ihnen studierten Fachgebiet. Ähnlich viele erreichen einen unmittelbaren Karriereaufstieg. All dies ist einer Studienmethodik zu verdanken, die ihre Wirksamkeit auf den Erwerb praktischer Fähigkeiten stützt, die für die berufliche Entwicklung absolut notwendig sind.

Google Partner Premier

Der amerikanische Technologieriese hat TECH mit dem Logo Google Partner Premier ausgezeichnet. Diese Auszeichnung, die nur 3% der Unternehmen weltweit erhalten, unterstreicht die effiziente, flexible und angepasste Erfahrung, die diese Universität den Studenten bietet. Die Anerkennung bestätigt nicht nur die maximale Präzision, Leistung und Investition in die digitalen Infrastrukturen der TECH, sondern positioniert diese Universität auch als eines der modernsten Technologieunternehmen der Welt.

Die von ihren Studenten am besten bewertete Universität

Das Bewertungsportal Global score hat TECH als die von ihren Studenten am besten bewertete Universität der Welt eingestuft. Dieses Bewertungsportal, das als das zuverlässigste und renommierteste gilt, weil es die Authentizität jeder veröffentlichten Meinung überprüft und bestätigt, hat TECH auf der Grundlage von mehr als 1000 erhaltenen Bewertungen mit 4,9 von 5 Punkten die höchste Bewertung gegeben. Diese Zahlen machen TECH zum absoluten Maßstab für internationale Universitäten.

03

Lehrplan

Die Lehrmaterialien dieses Weiterbildenden Masterstudiengangs in Secure Information Management wurden von einem Team von Experten für Cybersicherheit und Datenmanagement entwickelt. Auf diese Weise befasst sich der Lehrplan mit den wichtigsten digitalen Bedrohungen und den fortschrittlichsten Methoden für den Schutz und die Verwaltung von Informationen. Dadurch werden die Absolventen in die Lage versetzt, spezifische Risiken zu erkennen und wirksame Lösungen zu entwickeln, um die Datensicherheit in verschiedenen beruflichen Umgebungen zu gewährleisten. Der Lehrplan befasst sich auch mit den innovativsten Instrumenten des Sektors und fördert Strategien zum Schutz der digitalen Vermögenswerte von Organisationen.

Sie werden zum Schutz sensibler Daten und zur Schaffung sicherer Systeme beitragen, die die betriebliche Kontinuität von Unternehmen und Institutionen gewährleisten"

Modul 1. Datenanalytik in der Unternehmensorganisation

1.1. Business-Analyse
- 1.1.1. Business-Analyse
- 1.1.2. Datenstruktur
- 1.1.3. Phasen und Elemente

1.2. Datenanalytik im Unternehmen
- 1.2.1. *Dashboards* und KPI's nach Abteilungen
- 1.2.2. Operative, taktische und strategische Berichterstattung
- 1.2.3. Datenanalytik für jede Abteilung
  - 1.2.3.1. Marketing und Kommunikation
  - 1.2.3.2. Verkauf
  - 1.2.3.3. Kundendienst
  - 1.2.3.4. Einkauf
  - 1.2.3.5. Verwaltung
  - 1.2.3.6. Personalwesen
  - 1.2.3.7. Produktion
  - 1.2.3.8. IT

1.3. Marketing und Kommunikation
- 1.3.1. Zu messende KPIs, Anwendungen und Vorteile
- 1.3.2. Marketingsysteme und *Data Warehouse*
- 1.3.3. Implementierung einer Struktur zur Datenanalyse im Marketing
- 1.3.4. Marketing- und Kommunikationsplan
- 1.3.5. Strategien, Prognosen und Kampagnenmanagement

1.4. Kommerziell und Verkauf
- 1.4.1. Beiträge der Datenanalytik im kaufmännischen Bereich
- 1.4.2. Bedürfnisse der Verkaufsabteilung
- 1.4.3. Marktstudien

1.5. Kundendienst
- 1.5.1. Loyalität
- 1.5.2. Persönliche Qualität und emotionale Intelligenz
- 1.5.3. Kundenzufriedenheit

1.6. Einkauf
- 1.6.1. Datenanalytik für die Marktforschung
- 1.6.2. Datenanalytik für die Wettbewerbsforschung
- 1.6.3. Andere Anwendungen

1.7. Verwaltung
- 1.7.1. Bedürfnisse der Verwaltungssabteilung
- 1.7.2. *Data Warehouse* und finanzielle Risikoanalyse
- 1.7.3. *Data Warehouse* und finanzielle Risikoanalyse

1.8. Personalwesen
- 1.8.1. Personalwesen und Vorteile der Datenanalyse
- 1.8.2. Datenanalysetools im Personalwesen
- 1.8.3. Anwendung von Datenanalysen im Personalwesen

1.9. Produktion
- 1.9.1. Datenanalyse in einer Produktionsabteilung
- 1.9.2. Anwendungen
- 1.9.3. Vorteile

1.10. IT
- 1.10.1. IT-Abteilung
- 1.10.2. Datenanalytik und digitale Transformation
- 1.10.3. Innovation und Produktivität

Modul 2. Management und Bearbeitung von Daten und Informationen für die Datenwissenschaft

2.1. Statistik Variablen, Indizes und Kennziffern
- 2.1.1. Die Statistik
- 2.1.2. Statistische Dimensionen
- 2.1.3. Variablen, Indizes und Kennziffern

2.2. Daten-Typologie
- 2.2.1. Qualitative
- 2.2.2. Quantitative
- 2.2.3. Charakterisierung und Kategorien

2.3. Wissen über Daten aus Messungen
- 2.3.1. Maßnahmen zur Zentralisierung
- 2.3.2. Maßnahmen zur Streuung
- 2.3.3. Korrelation

2.4. Wissen über Daten aus Diagrammen
  2.4.1. Visualisierung nach Datentyp
  2.4.2. Interpretation von grafischen Informationen
  2.4.3. Anpassung von Grafiken mit R
2.5. Wahrscheinlichkeit
  2.5.1. Wahrscheinlichkeit
  2.5.2. Wahrscheinlichkeitsfunktion
  2.5.3. Verteilungen
2.6. Datenerhebung
  2.6.1. Methodik der Erhebung
  2.6.2. Erhebungsinstrumente
  2.6.3. Kanäle für die Erhebung
2.7. Datenbereinigung
  2.7.1. Phasen der Datenbereinigung
  2.7.2. Qualität der Daten
  2.7.3. Datenmanipulation (mit R)
2.8. Datenanalyse, Interpretation und Bewertung der Ergebnisse
  2.8.1. Statistische Maßnahmen
  2.8.2. Beziehungsindizes
  2.8.3. *Data Mining*
2.9. Datenlager (*Datawarehouse*)
  2.9.1. Elemente
  2.9.2. Design
2.10. Verfügbarkeit von Daten
  2.10.1. Zugang
  2.10.2. Nützlichkeit
  2.10.3. Sicherheit

Modul 3. IoT-Geräte und -Plattformen als Grundlage für die Datenwissenschaft

3.1. *Internet of Things*
  3.1.1. Internet der Zukunft, *Internet of Things*
  3.1.2. Industrielles Internet-Konsortium
3.2. Referenzarchitektur
  3.2.1. Die Referenzarchitektur
  3.2.2. Ebenen
  3.2.3. Komponenten
3.3. Sensoren und IoT-Geräte
  3.3.1. Hauptkomponenten
  3.3.2. Sensoren und Aktuatoren
3.4. Kommunikation und Protokolle
  3.4.1. Protokolle. OSI-Modell
  3.4.2. Kommunikationstechnologien
3.5. *Cloud*-Plattformen für IoT und IIoT
  3.5.1. Allzweck-Plattformen
  3.5.2. Industrielle Plattformen
  3.5.3. Open-Source-Plattformen
3.6. Datenmanagement in IoT-Plattformen
  3.6.1. Mechanismen zur Datenverwaltung. Offene Daten
  3.6.2. Datenaustausch und Visualisierung
3.7. IoT-Sicherheit
  3.7.1. Sicherheitsanforderungen und -bereiche
  3.7.2. IIoT-Sicherheitsstrategien
3.8. IoT-Anwendungen
  3.8.1. Intelligente Städte
  3.8.2. Gesundheit und Fitness
  3.8.3. Intelligentes Zuhause
  3.8.4. Andere Anwendungen
3.9. IIoT-Anwendungen
  3.9.1. Herstellung
  3.9.2. Transport
  3.9.3. Energie
  3.9.4. Landwirtschaft und Viehzucht
  3.9.5. Andere Sektoren
3.10. Industrie 4.0.
  3.10.1. IoRT *(Internet of Robotics Things)*
  3.10.2. 3D-Additive-Fertigung
  3.10.3. *Big Data Analytics*

Modul 4. Grafische Darstellung für die Datenanalyse

4.1. Explorative Analyse
- 4.1.1. Repräsentation für die Informationsanalyse
- 4.1.2. Der Wert der grafischen Darstellung
- 4.1.3. Neue Paradigmen der grafischen Darstellung

4.2. Optimierung für Datenwissenschaft
- 4.2.1. Farbpalette und Design
- 4.2.2. Gestalt in der grafischen Darstellung
- 4.2.3. Zu vermeidende Fehler und Tipps

4.3. Grundlegende Datenquellen
- 4.3.1. Für die Qualitätsdarstellung
- 4.3.2. Für die Mengendarstellung
- 4.3.3. Für die Zeitdarstellung

4.4. Komplexe Datenquellen
- 4.4.1. Dateien, Listen und Datenbanken
- 4.4.2. Offene Daten
- 4.4.3. Kontinuierlich generierte Daten

4.5. Arten von Grafiken
- 4.5.1. Grundlegende Darstellungen
- 4.5.2. Blockdarstellung
- 4.5.3. Darstellung für die Ausbreitungsanalyse
- 4.5.4. Zirkuläre Darstellungen
- 4.5.5. Blasen-Darstellungen
- 4.5.6. Geografische Darstellung

4.6. Arten der Visualisierung
- 4.6.1. Vergleichend und relational
- 4.6.2. Vertrieb
- 4.6.3. Hierarchisch

4.7. Berichtsentwurf mit grafischer Darstellung
- 4.7.1. Anwendung von Diagrammen in Marketingberichten
- 4.7.2. Anwendung von Diagrammen in *Dashboards* und KPI
- 4.7.3. Anwendung von Grafiken in strategischen Plänen
- 4.7.4. Andere Verwendungen: Wissenschaft, Gesundheit, Wirtschaft

4.8. Grafisches Geschichtenerzählen
- 4.8.1. Grafisches Geschichtenerzählen
- 4.8.2. Evolution
- 4.8.3. Nützlichkeit

4.9. Visualisierungsorientierte Tools
- 4.9.1. Erweiterte Tools
- 4.9.2. Online-Software
- 4.9.3. *Open Source*

4.10. Neue Technologien zur Datenvisualisierung
- 4.10.1. Systeme zur Virtualisierung der Realität
- 4.10.2. Systeme für Realitätserweiterung und -verbesserung
- 4.10.3. Intelligente Systeme

Modul 5. Tools der Datenwissenschaft

5.1. Datenwissenschaft
- 5.1.1. Datenwissenschaft
- 5.1.2. Fortgeschrittene Tools für den Datenwissenschaftler

5.2. Daten, Informationen und Wissen
- 5.2.1. Daten, Informationen und Wissen
- 5.2.2. Datentypen
- 5.2.3. Datenquellen

5.3. Von Daten zu Informationen
- 5.3.1. Analyse der Daten
- 5.3.2. Arten der Analyse
- 5.3.3. Extraktion von Informationen aus einem *Dataset*

5.4. Extraktion von Informationen durch Visualisierung
- 5.4.1. Visualisierung als Analyseinstrument
- 5.4.2. Visualisierungsmethoden
- 5.4.3. Visualisierung eines Datensatzes

5.5. Qualität der Daten
- 5.5.1. Datenqualität
- 5.5.2. Datenbereinigung
- 5.5.3. Grundlegende Datenvorverarbeitung

5.6. *Dataset*
- 5.6.1. *Dataset*-Anreicherung
- 5.6.2. Der Fluch der Dimensionalität
- 5.6.3. Ändern unseres Datensatzes

5.7. Ungleichgewicht
- 5.7.1. Ungleichgewicht der Klassen
- 5.7.2. Techniken zur Begrenzung von Ungleichgewichten
- 5.7.3. *Dataset*-Abgleich

5.8. Unüberwachte Modelle
- 5.8.1. Unüberwachtes Modell
- 5.8.2. Methoden
- 5.8.3. Klassifizierung mit unüberwachten Modellen

5.9. Überwachte Modelle
- 5.9.1. Überwachtes Modell
- 5.9.2. Methoden
- 5.9.3. Klassifizierung mit überwachten Modellen

5.10. Tools und bewährte Verfahren
- 5.10.1. Bewährte Praktiken für einen Datenwissenschaftler
- 5.10.2. Das beste Modell
- 5.10.3. Nützliche Tools

Modul 6. *Data Mining* - Auswahl, Vorverarbeitung und Transformation

6.1. Statistische Inferenz
- 6.1.1. Deskriptive Statistik vs. Statistische Inferenz
- 6.1.2. Parametrische Verfahren
- 6.1.3. Nichtparametrische Verfahren

6.2. Explorative Analyse
- 6.2.1. Deskriptive Analyse
- 6.2.2. Visualisierung
- 6.2.3. Vorbereitung der Daten

6.3. Vorbereitung der Daten
- 6.3.1. Datenintegration und -bereinigung
- 6.3.2. Normalisierung der Daten
- 6.3.3. Attribute umwandeln

6.4. Verlorene Werte
- 6.4.1. Umgang mit verlorenen Werten
- 6.4.2. Maximum-Likelihood-Imputationsmethoden
- 6.4.3. Imputation verlorener Werte durch maschinelles Lernen

6.5. Datenrauschen
- 6.5.1. Lärmklassen und Attribute
- 6.5.2. Rauschfilterung
- 6.5.3. Rauscheffekt

6.6. Der Fluch der Dimensionalität
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Multidimensionale Datenreduktion

6.7. Kontinuierliche zu diskreten Attributen
- 6.7.1. Kontinuierliche versus diskrete Daten
- 6.7.2. Prozess der Diskretisierung

6.8. Daten
- 6.8.1. Datenauswahl
- 6.8.2. Perspektiven und Auswahlkriterien
- 6.8.3. Methoden der Auswahl

6.9. Auswahl der Instanzen
- 6.9.1. Methoden für die Instanzauswahl
- 6.9.2. Auswahl von Prototypen
- 6.9.3. Erweiterte Methoden für die Instanzauswahl

6.10. Vorverarbeitung von Daten in *Big-Data*-Umgebungen
- 6.10.1. *Big Data*
- 6.10.2. „Klassische" versus massive Vorbearbeitung
- 6.10.3. *Smart Data*

Modul 7. Vorhersagbarkeit und Analyse von stochastischen Phänomenen

7.1. Zeitreihen
- 7.1.1. Zeitreihen
- 7.1.2. Nützlichkeit und Anwendbarkeit
- 7.1.3. Verwandte Kasuistik

7.2. Die Zeitreihen
- 7.2.1. Saisonaler Trend von ZR
- 7.2.2. Typische Variationen
- 7.2.3. Residuale Analyse

7.3. Typologien
- 7.3.1. Stationär
- 7.3.2. Nicht stationär
- 7.3.3. Transformationen und Anpassungen

7.4. Schemata für Zeitreihen
- 7.4.1. Additives Schema (Modell)
- 7.4.2. Multiplikatives Schema (Modell)
- 7.4.3. Verfahren zur Bestimmung der Art des Modells

7.5. Grundlegende Methoden des *Forecast*
- 7.5.1. Durchschnitt
- 7.5.2. *Naive*
- 7.5.3. *Saisonal Naive*
- 7.5.4. Vergleich der Methoden

7.6. Residuale Analyse
- 7.6.1. Autokorrelation
- 7.6.2. ACF der Residuen
- 7.6.3. Korrelationstest

7.7. Regression im Kontext von Zeitreihen
- 7.7.1. ANOVA
- 7.7.2. Grundlagen
- 7.7.3. Praktische Anwendung

7.8. Prädiktive Zeitreihenmodelle
- 7.8.1. ARIMA
- 7.8.2. Exponentiale Glättung

7.9. Zeitreihenmanipulation und -analyse mit R
- 7.9.1. Vorbereitung der Daten
- 7.9.2. Muster-Identifizierung
- 7.9.3. Modell-Analyse
- 7.9.4. Vorhersage

7.10. Grafische Analyse kombiniert mit R
- 7.10.1. Typische Situationen
- 7.10.2. Praktische Anwendung zum Lösen einfacher Probleme
- 7.10.3. Praktische Anwendung für fortgeschrittene Problemlösungen

Modul 8. Design und Entwicklung von intelligenten Systemen

8.1. Vorverarbeitung der Daten
- 8.1.1. Vorverarbeitung der Daten
- 8.1.2. Datenumwandlung
- 8.1.3. *Data Mining*

8.2. Automatisches Lernen
- 8.2.1. Überwachtes und unüberwachtes Lernen
- 8.2.2. Lernen durch Verstärkung
- 8.2.3. Andere Lernparadigmen

8.3. Klassifizierungsalgorithmen
- 8.3.1. Induktives automatisches Lernen
- 8.3.2. SVM und KNN
- 8.3.3. Metriken und Punktzahlen für die Rangliste

8.4. Regressionsalgorithmen
- 8.4.1. Lineare Regression, logistische Regression und nichtlineare Modelle
- 8.4.2. Zeitreihen
- 8.4.3. Regressionsmetriken und -werte

8.5. *Clustering*-Algorithmen
- 8.5.1. Hierarchische *Clustering*-Techniken
- 8.5.2. Partitionelle *Clustering*-Techniken
- 8.5.3. *Clustering*-Metriken und -Bewertungen

8.6. Assoziationsregel-Techniken
- 8.6.1. Methoden zur Extraktion von Regeln
- 8.6.2. Metriken und Punktzahlen für Assoziationsregel-Algorithmen

8.7. Erweiterte Klassifizierungstechniken. Multiklassifizierer
- 8.7.1. *Bagging*-Algorithmen
- 8.7.2. *Random Forests*-Sortierer
- 8.7.3. *Boosting* für Entscheidungsbäume

8.8. Probabilistische grafische Modelle
- 8.8.1. Probabilistische Modelle
- 8.8.2. Bayes'sche Netzwerke. Eigenschaften, Darstellung und Parametrisierung
- 8.8.3. Andere probabilistische grafische Modelle

8.9. Neuronale Netze
- 8.9.1. Maschinelles Lernen mit künstlichen neuronalen Netzen
- 8.9.2. *Feedforward*-Netzwerke

8.10. Tiefes Lernen
- 8.10.1. Tiefe *Feedforward*-Netzwerke
- 8.10.2. Faltungsneuronale Netze und Sequenzmodelle
- 8.10.3. Tools für die Implementierung tiefer neuronaler Netze

Modul 9. Datenintensive Architekturen und Systeme

9.1. Nicht funktionale Anforderungen. Säulen der *Big-Data*-Anwendungen
- 9.1.1. Verlässlichkeit
- 9.1.2. Anpassungsfähigkeit
- 9.1.3. Instandhaltbarkeit

9.2. Datenmodelle
- 9.2.1. Relationales Modell
- 9.2.2. Dokumentarisches Modell
- 9.2.3. Graph-Datenmodell

9.3. Datenbanken. Verwaltung der Speicherung und des Abrufs von Daten
- 9.3.1. Hash-Index
- 9.3.2. Strukturierte Speicherung von Logs
- 9.3.3. B-Bäume

9.4. Datenverschlüsselungsformate
- 9.4.1. Sprachspezifische Formate
- 9.4.2. Standardisierte Formate
- 9.4.3. Binäre Kodierungsformate
- 9.4.4. Prozessübergreifender Datenfluss

9.5. Replikation
- 9.5.1. Ziele der Replikation
- 9.5.2. Replikationsmodelle
- 9.5.3. Probleme mit der Replikation

9.6. Verteilte Transaktionen
- 9.6.1. Transaktion
- 9.6.2. Protokolle für verteilte Transaktionen
- 9.6.3. Serialisierbare Transaktionen

9.7. Aufteilung
- 9.7.1. Formulare unterteilen
- 9.7.2. Interaktion von Sekundärindex und Partitionierung
- 9.7.3. Partitionierung neu ausbalancieren

9.8. *Offline*-Datenverarbeitung
- 9.8.1. Stapelverarbeitung
- 9.8.2. Verteilte Dateisysteme
- 9.8.3. *MapReduce*

9.9. Datenverarbeitung in Echtzeit
- 9.9.1. Arten von *Message Broker*
- 9.9.2. Darstellung von Datenbanken als Datenströme
- 9.9.3. Verarbeitung von Datenströmen

9.10. Praktische Anwendungen im Unternehmen
- 9.10.1. Konsistenz bei der Lektüre
- 9.10.2. Ganzheitlicher Ansatz für Daten
- 9.10.3. Skalierung eines verteilten Dienstes

Modul 10. Praktische Anwendung der Datenwissenschaft in Geschäftsbereichen

10.1. Gesundheitssektor
- 10.1.1. Auswirkungen von KI und Datenanalyse im Gesundheitssektor
- 10.1.2. Chancen und Herausforderungen

10.2. Risiken und Trends in der Gesundheitsbranche
- 10.2.1. Verwendung im Gesundheitssektor
- 10.2.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.3. Finanzdienstleistungen
- 10.3.1. Auswirkungen von KI und Datenanalyse auf den Finanzdienstleistungssektor
- 10.3.2. Verwendung bei Finanzdienstleistungen
- 10.3.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.4. Retail
- 10.4.1. Auswirkungen von KI und Datenanalyse auf den *Retail*-Sektor
- 10.4.2. Verwendung im *Retail*
- 10.4.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.5. Industrie 4.0.
- 10.5.1. Auswirkungen von KI und Datenanalyse in der Industrie 4.0
- 10.5.2. Einsatz in der Industrie 4.0

10.6. Risiken und Trends in der Industrie 4.0
- 10.6.1. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.7. Öffentliche Verwaltung
- 10.7.1. Auswirkungen von KI und Datenanalyse in der öffentlichen Verwaltung
- 10.7.2. Verwendung in der öffentlichen Verwaltung
- 10.7.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.8. Bildung
- 10.8.1. Auswirkungen von KI und Datenanalyse im Bildungswesen
- 10.8.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.9. Forst- und Landwirtschaft
- 10.9.1. Auswirkungen von KI und Datenanalyse auf Forst- und Landwirtschaft
- 10.9.2. Verwendung in Forst- und Landwirtschaft
- 10.9.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

10.10. Personalwesen
- 10.10.1. Auswirkungen von KI und Datenanalyse auf das Personalmanagement
- 10.10.2. Praktische Anwendungen in der Geschäftswelt
- 10.10.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

Modul 11. Cyberintelligenz und Cybersicherheit

11.1. Cyberintelligenz
- 11.1.1. Cyberintelligenz
  - 11.1.1.1. Die Intelligenz
    - 11.1.1.1.1. Intelligenz-Zyklus
  - 11.1.1.2. Cyberintelligenz
  - 11.1.1.3. Cyberintelligenz und Cybersicherheit
- 11.1.2. Der Informationsanalyst
  - 11.1.2.1. Die Rolle des Informationsanalysten
  - 11.1.2.2. Voreingenommenheit des Informationsanalysten bei der Bewertung von Aktivitäten

11.2. Cybersicherheit
- 11.2.1. Schichten der Sicherheit
- 11.2.2. Identifizierung von Cyber-Bedrohungen
  - 11.2.2.1. Externe Bedrohungen
  - 11.2.2.2. Interne Bedrohungen
- 11.2.3. Nachteilige Maßnahmen
  - 11.2.3.1. *Social Engineering*
  - 11.2.3.2. Häufig verwendete Methoden

11.3. Intelligente Tools und Techniken
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Linux-Distributionen und -Tools
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Methoden der Bewertung
- 11.4.1. Informationsanalyse
- 11.4.2. Techniken zur Organisation der erworbenen Informationen
- 11.4.3. Verlässlichkeit und Glaubwürdigkeit von Informationsquellen
- 11.4.4. Methodologien der Analyse
- 11.4.5. Präsentation der Informationsanalyse

11.5. Audits und Dokumentation
- 11.5.1. Das IT-Sicherheitsaudit
- 11.5.2. Dokumentation und Berechtigungen für Audits
- 11.5.3. Arten von Audits
- 11.5.4. Lieferbare
  - 11.5.4.1. Technischer Bericht
  - 11.5.4.2. Bericht für die Geschäftsführung

11.6. Anonymität im Netz
- 11.6.1. Nutzung der Anonymität
- 11.6.2. Anonymisierungstechniken (Proxy, VPN)
- 11.6.3. TOR, Freenet und IP2-Netzwerke

11.7. Bedrohungen und Arten von Sicherheit
- 11.7.1. Arten von Bedrohungen
- 11.7.2. Physische Sicherheit
- 11.7.3. Netzwerksicherheit
- 11.7.4. Logische Sicherheit
- 11.7.5. Sicherheit von Webanwendungen
- 11.7.6. Sicherheit für mobile Geräte

11.8. Regulierung und *Compliance*
- 11.8.1. Datenschutz-Grundverordnung
- 11.8.2. Die nationale Cybersicherheitsstrategie 2019
- 11.8.3. ISO 27000-Familie
- 11.8.4. NIST Cybersecurity Framework
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. *Cloud*-Vorschriften
- 11.8.8. SOX
- 11.8.9. ICP

11.9. Risikoanalyse und Metriken
- 11.9.1. Umfang der Risiken
- 11.9.2. Vermögenswerte
- 11.9.3. Bedrohungen
- 11.9.4. Schwachstellen
- 11.9.5. Risikobewertung
- 11.9.6. Risikobehandlung

11.10. Einschlägige Stellen für Cybersicherheit
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Modul 12. Host-Sicherheit

12.1. Sicherheitskopien
- 12.1.1. Strategien zur Datensicherung
- 12.1.2. Tools für Windows
- 12.1.3. Tools für Linux
- 12.1.4. Tools für MacOS

12.2. Benutzer-Antivirus
- 12.2.1. Arten von Antivirenprogrammen
- 12.2.2. Antivirus für Windows
- 12.2.3. Antivirus für Linux
- 12.2.4. Antivirus für MacOS
- 12.2.5. Antivirus für Smartphones

12.3. Eindringlingsdetektoren - HIDS
- 12.3.1. Methoden zur Erkennung von Eindringlingen
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. Lokale *Firewall*
- 12.4.1. *Firewalls* für Windows
- 12.4.2. *Firewalls* für Linux
- 12.4.3. *Firewalls* für MacOS

12.5. Passwortmanager
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *StickyPassword*
- 12.5.5. *RoboForm*

12.6. *Phishing*-Detektoren
- 12.6.1. Manuelle *Phishing*-Erkennung
- 12.6.2. *Anti-Phishing*-Tools

12.7. *Spyware*
- 12.7.1. Vermeidungsmechanismen
- 12.7.2. *Anti-Spyware*-Tools

12.8. *Tracker*
- 12.8.1. Maßnahmen zum Schutz des Systems
- 12.8.2. *Anti-Tracking*-Tools

12.9. EDR - *End Point Detection and Response*
- 12.9.1. Verhalten des EDR-Systems
- 12.9.2. Unterschiede zwischen EDR und Anti-Virus
- 12.9.3. Die Zukunft der EDR-Systeme

12.10. Kontrolle über die Software-Installation
- 12.10.1. Repositorien und Software-Speicher
- 12.10.2. Listen mit erlaubter oder verbotener Software
- 12.10.3. Update-Kriterien
- 12.10.4. Berechtigungen für die Software-Installation

Modul 13. Netzwerksicherheit (Perimeter)

13.1. Systeme zur Erkennung und Abwehr von Bedrohungen
- 13.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 13.1.2. Aktuelle Verteidigungssysteme*: Defense in Depth* und SOC
- 13.1.3. Aktuelle Netzwerkarchitekturen
- 13.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
  - 13.1.4.1. Netzwerkbasierte Systeme
  - 13.1.4.2. Host-basierte Systeme
  - 13.1.4.3. Zentralisierte Systeme
- 13.1.5. Kommunikation und Erkennung von Instanzen/*Hosts*, Containern und *Serverless*

13.2. *Firewall*
- 13.2.1. Arten von *Firewalls*
- 13.2.2. Angriffe und Schadensbegrenzung
- 13.2.3. Gängige *Firewalls* in Kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables und iptables
  - 13.2.3.3. *Firewalld*
- 13.2.4. Erkennungssysteme auf der Grundlage von Systemlogs
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* und *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
- 13.3.1. Angriffe auf IDS/IPS
- 13.3.2. IDS/IPS-Systeme
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewalls* der nächsten Generation (NGFW)
- 13.4.1. Unterschiede zwischen NGFW und traditionellen Firewalls
- 13.4.2. Kernkapazitäten
- 13.4.3. Business-Lösungen
- 13.4.4. Firewalls für *Cloud*-Dienste
  - 13.4.4.1. *Cloud* VPC-Architektur
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Arten von Proxys
- 13.5.2. Proxy-Nutzung. Vor- und Nachteile

13.6. Antivirus-Engines
- 13.6.1. Allgemeiner Kontext von *Malware* und IOCs
- 13.6.2. Probleme mit Anti-Viren-Programmen

13.7. Mailschutzsysteme
- 13.7.1. Antispam
  - 13.7.1.1. Schwarze und weiße Listen
  - 13.7.1.2. Bayessche Filter
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Komponenten und Architektur
- 13.8.2. Korrelationsregeln und Anwendungsfälle
- 13.8.3. Aktuelle Herausforderungen von SIEM-Systemen

13.9. SOAR
- 13.9.1. SOAR und SIEM: Feinde oder Verbündete?
- 13.9.2. Die Zukunft der SOAR-Systeme

13.10. Andere netzwerkbasierte Systeme
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots und HoneyNets
- 13.10.4. CASB

Modul 14. Smartphone-Sicherheit

14.1. Die Welt der mobilen Geräte
- 14.1.1. Arten von mobilen Plattformen
- 14.1.2. IOS-Geräte
- 14.1.3. Android-Geräte

14.2. Verwaltung der mobilen Sicherheit
- 14.2.1. OWASP-Projekt für mobile Sicherheit
  - 14.2.1.1. Top 10 Schwachstellen
- 14.2.2. Kommunikation, Netzwerke und Verbindungsarten

14.3. Das mobile Gerät in der Unternehmensumgebung
- 14.3.1. Risiken
- 14.3.2. Sicherheitsrichtlinien
- 14.3.3. Geräteüberwachung
- 14.3.4. Verwaltung mobiler Geräte (MDM)

14.4. Datenschutz und Datensicherheit
- 14.4.1. Informationsstände
- 14.4.2. Datenschutz und Vertraulichkeit
  - 14.4.2.1. Zugriffsrechte
  - 14.4.2.2. Verschlüsselung
- 14.4.3. Sichere Speicherung von Daten
  - 14.4.3.1. Sichere Speicherung auf iOS
  - 14.4.3.2. Sichere Speicherung auf Android
- 14.4.4. Bewährte Praktiken bei der Applikationsentwicklung

14.5. Schwachstellen und Angriffsvektoren
- 14.5.1. Schwachstellen
- 14.5.2. Angriffsvektoren
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Exfiltration von Daten
  - 14.5.2.3. Datenmanipulation

14.6. Wichtigste Bedrohungen
- 14.6.1. Ungezwungener Benutzer
- 14.6.2. *Malware*
  - 14.6.2.1. Arten von *Malware*
- 14.6.3. *Social Engineering*
- 14.6.4. Datenleck
- 14.6.5. Datendiebstahl
- 14.6.6. Ungesicherte *WLAN*-Netzwerke
- 14.6.7. Veraltete Software
- 14.6.8. Bösartige Anwendungen
- 14.6.9. Unsichere Passwörter
- 14.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen
- 14.6.11. Physischer Zugang
- 14.6.12. Verlust oder Diebstahl des Geräts
- 14.6.13. Impersonation (Integrität)
- 14.6.14. Schwache oder defekte Kryptographie
- 14.6.15. *Denial of Service* (DoS)

14.7. Große Angriffe
- 14.7.1. *Phishing*-Angriffe
- 14.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
- 14.7.3. *Smishing*-Angriffe
- 14.7.4. *Criptojacking*-Angriffe
- 14.7.5. *Man in The Middle*

14.8. *Hacking*
- 14.8.1. *Rooting und Jailbreaking*
- 14.8.2. Anatomie eines mobilen Angriffs
  - 14.8.2.1. Ausbreitung der Bedrohung
  - 14.8.2.2. Installation von *Malware* auf dem Gerät
  - 14.8.2.3. Persistenz
  - 14.8.2.4. Ausführung der *Payload* und Extraktion von Informationen
- 14.8.3. *Hacking* auf iOS-Geräten: Mechanismen und Tools
- 14.8.4. *Hacking* auf Android-Geräten: Mechanismen und Tools

14.9. Penetrationstests
- 14.9.1. iOS *Pentesting*
- 14.9.2. *Android PenTesting*
- 14.9.3. Werkzeuge

14.10. Schutz und Sicherheit
- 14.10.1. Sicherheitseinstellungen
  - 14.10.1.1. Auf iOS-Geräten
  - 14.10.1.2. Auf Android-Geräten
- 14.10.2. Sicherheitsmaßnahmen
- 14.10.3. Schutz-Tools

Modul 15. IoT-Sicherheit

15.1. Geräte
- 15.1.1. Arten von Geräten
- 15.1.2. Standardisierte Architekturen
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Anwendungsprotokolle
- 15.1.4. Konnektivitätstechnologien

15.2. IoT-Geräte. Anwendungsbereiche
- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Transport
- 15.2.4. *Wearables*
- 15.2.5. Gesundheitssektor
- 15.2.6. IIoT

15.3. Kommunikationsprotokolle
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. *SmartHome*
- 15.4.1. Hausautomatisierung
- 15.4.2. Netzwerke
- 15.4.3. Haushaltsgeräte
- 15.4.4. Überwachung und Sicherheit

15.5. *SmartCity*
- 15.5.1. Beleuchtung
- 15.5.2. Meteorologie
- 15.5.3. Sicherheit

15.6. Transport
- 15.6.1. Standort
- 15.6.2. Zahlungen leisten und Dienstleistungen in Anspruch nehmen
- 15.6.3. Konnektivität

15.7. *Wearables*
- 15.7.1. Intelligente Kleidung
- 15.7.2. Intelligenter Schmuck
- 15.7.3. Intelligente Uhren

15.8. Gesundheitssektor
- 15.8.1. Training/Herzfrequenzüberwachung
- 15.8.2. Überwachung von Patienten und älteren Menschen
- 15.8.3. Implantierbare Geräte
- 15.8.4. Chirurgische Roboter

15.9. Konnektivität
- 15.9.1. *WLAN/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Eingebettete Konnektivität

15.10. Sicherung
- 15.10.1. Dedizierte Netzwerke
- 15.10.2. Passwortmanager
- 15.10.3. Verwendung von verschlüsselten Protokollen
- 15.10.4. Tipps für die Verwendung

Modul 16. Ethisches *Hacking*

16.1. Arbeitsumgebung
- 16.1.1. Linux-Distributionen
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Virtualisierungssysteme
- 16.1.3. *Sandbox*
- 16.1.4. Einsatz von Labors

16.2. Methoden
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. *Open Source Intelligence* (OSINT)
- 16.3.2. Suche nach Datenschutzverletzungen und Schwachstellen
- 16.3.3. Verwendung von passiven Tools

16.4. Netzwerk-Scans
- 16.4.1. Tools zum Scannen
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Andere Scan-Tools
- 16.4.2. Scanning-Techniken
- 16.4.3. Techniken zur Umgehung von *Firewalls* und IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Netzwerk-Diagramme

16.5. Aufzählung
- 16.5.1. SMTP-Aufzählung
- 16.5.2. DNS-Aufzählung
- 16.5.3. NetBIOS- und Samba-Aufzählung
- 16.5.4. LDAP-Aufzählung
- 16.5.5. SNMP-Aufzählung
- 16.5.6. Andere Aufzählungstechniken

16.6. Scannen auf Schwachstellen
- 16.6.1. Lösungen zum Scannen auf Schwachstellen
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Systeme zur Bewertung von Schwachstellen
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Angriffe auf drahtlose Netzwerke
- 16.7.1. Methodik zum *Hacking* drahtloser Netzwerke
  - 16.7.1.1. WLAN Discovery
  - 16.7.1.2. Verkehrsanalyse
  - 16.7.1.3. *Aircrack*-Angriffe
    - 16.7.1.3.1. WEP-Angriffe
    - 16.7.1.3.2. WPA/WPA2-Angriffe
  - 16.7.1.4. *Evil-Twin*-Angriffe
  - 16.7.1.5. WPS-Angriffe
  - 16.7.1.6. *Jamming*
- 16.7.2. Tools für drahtlose Sicherheit

16.8. *Hacking* von Webservern
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Ausnutzung von Schwachstellen
- 16.9.1. Verwendung von bekannten *Exploits*
- 16.9.2. Verwendung von *Metasploit*
- 16.9.3. Verwendung von *Malware*
  - 16.9.3.1. Definition und Umfang
  - 16.9.3.2. Generierung von *Malware*
  - 16.9.3.3. Umgehung von Anti-Virus-Lösungen

16.10. Persistenz
- 16.10.1. Installation von Rootkits
- 16.10.2. Verwendung von Ncat
- 16.10.3. Verwendung von geplanten Aufgaben für Backdoors
- 16.10.4. Benutzer erstellen
- 16.10.5. HIDS aufspüren

Modul 17. *Reverse Engineering*

17.1. *Compiler*
- 17.1.1. Arten von Code
- 17.1.2. *Compiler*-Phasen
- 17.1.3. Symboltabelle
- 17.1.4. Fehler-Handler
- 17.1.5. GCC Compiler

17.2. Arten der *Compiler*-Analyse
- 17.2.1. Lexikalische Analyse
  - 17.2.1.1. Terminologie
  - 17.2.1.2. Lexikalische Komponenten
  - 17.2.1.3. LEX. Lexikalischer Analysator
- 17.2.2. Syntaktische Analyse
  - 17.2.2.1. Kontextfreie Grammatiken
  - 17.2.2.2. Arten des *Parsing*
    - 17.2.2.2.1. Top-down-*Parsing*
    - 17.2.2.2.2. Bottom-up-*Parsing*
  - 17.2.2.3. Syntaktische Bäume und Ableitungen
  - 17.2.2.4. Arten von *Parsern*
    - 17.2.2.4.1. LR-*Parser* (*Left to Right*)
    - 17.2.2.4.2. LALR-*Parser*
- 17.2.3. Semantische Analyse
  - 17.2.3.1. Attribut-Grammatiken
  - 17.2.3.2. S-Attribute
  - 17.2.3.3. L-Attribute

17.3. Montage-Datenstrukturen
- 17.3.1. Variablen
- 17.3.2. Arrays
- 17.3.3. Zeiger
- 17.3.4. Strukturen
- 17.3.5. Objekte

17.4. *Assembly-Code*-Strukturen
- 17.4.1. Auswahl-Strukturen
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Iterations-Strukturen
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Verwendung des Break
- 17.4.3. Funktionen

17.5. x86-Hardware-Architektur
- 17.5.1. x86-Prozessorarchitektur
- 17.5.2. x86-Datenstrukturen
- 17.5.3. x86-Codestrukturen

17.6. ARM-Hardware-Architektur
- 17.6.1. ARM-Prozessorarchitektur
- 17.6.2. ARM-Datenstrukturen
- 17.6.3. ARM-Codestrukturen

17.7. Statische Codeanalyse
- 17.7.1. *Disassembler*
- 17.7.2. IDA
- 17.7.3. Code-Rekonstrukteure

17.8. Dynamische Codeanalyse
- 17.8.1. Verhaltensanalyse
  - 17.8.1.1. Kommunikation
  - 17.8.1.2. Überwachung
- 17.8.2. Linux-Code-Debugger
- 17.8.3. Windows-Code-Debugger

17.9. *Sandbox*
- 17.9.1. *Sandbox*-Architektur
- 17.9.2. *Sandbox*-Umgehung
- 17.9.3. Erkennungstechniken
- 17.9.4. Ausweichtechniken
- 17.9.5. Gegenmaßnahmen

17.9.6. *Sandbox* in Linux
17.9.7. *Sandbox* in Windows
17.9.8. *Sandbox* in MacOS
17.9.9. *Sandbox* in Android
17.10. *Malware*-Analyse
17.10.1. Methoden zur Analyse des *Malware*
17.10.2. Techniken zur Verschleierung von *Malware*
17.10.2.1. Ausführbare Verschleierung
17.10.2.2. Einschränkung der Ausführungsumgebungen
17.10.3. Tools zur Analyse des *Malware*

Modul 18. Sichere Entwicklung

18.1. Sichere Entwicklung
18.1.1. Qualität, Funktionalität und Sicherheit
18.1.2. Vertraulichkeit, Integrität und Verfügbarkeit
18.1.3. Lebenszyklus der Softwareentwicklung
18.2. Phase der Anforderungen
18.2.1. Kontrolle der Authentifizierung
18.2.2. Kontrolle von Rollen und Privilegien
18.2.3. Risikoorientierte Anforderungen
18.2.4. Genehmigung von Privilegien
18.3. Analyse- und Entwurfsphasen
18.3.1. Komponentenzugriff und Systemverwaltung
18.3.2. Prüfpfade
18.3.3. Sitzungsmanagement
18.3.4. Historische Daten
18.3.5. Angemessene Fehlerbehandlung
18.3.6. Trennung der Funktionen
18.4. Phase der Implementierung und Kodierung
18.4.1. Absicherung der Entwicklungsumgebung
18.4.2. Ausarbeitung der technischen Dokumentation
18.4.3. Sichere Kodierung
18.4.4. Sicherheit der Kommunikation
18.5. Gute sichere Kodierungspraktiken
18.5.1. Validierung von Eingabedaten
18.5.2. Verschlüsselung der Ausgabedaten
18.5.3. Programmierstil
18.5.4. Handhabung des Änderungsprotokolls
18.5.5. Kryptographische Praktiken
18.5.6. Fehler- und Protokollverwaltung
18.5.7. Dateiverwaltung
18.5.8. Speicherverwaltung
18.5.9. Standardisierung und Wiederverwendung von Sicherheitsfunktionen
18.6. Vorbereitung von Servern und *Hardening*
18.6.1. Verwaltung von Benutzern, Gruppen und Rollen auf dem Server
18.6.2. Software-Installation
18.6.3. *Hardening* des Servers
18.6.4. Robuste Konfiguration der Anwendungsumgebung
18.7. DB-Vorbereitung und *Hardening*
18.7.1. Optimierung der DB-Engine
18.7.2. Erstellung eines eigenen Benutzers für die Anwendung
18.7.3. Zuweisung der erforderlichen Berechtigungen an den Benutzer
18.7.4. *Hardening* der DB
18.8. Testphase
18.8.1. Qualitätskontrolle bei Sicherheitskontrollen
18.8.2. Stufenweise Code-Inspektion
18.8.3. Überprüfung der Konfigurationsverwaltung
18.8.4. Black-Box-Tests
18.9. Vorbereitungen für den Übergang zur Produktion
18.9.1. Änderungskontrolle durchführen
18.9.2. Durchführen der Produktionsumstellung
18.9.3. *Rollback*-Prozedur durchführen
18.9.4. Tests in der Vorproduktionsphase
18.10. Erhaltungsphase
18.10.1. Risikobasierte Versicherung
18.10.2. White-Box-Tests zur Wartung der Sicherheit
18.10.3. Black-Box-Tests zur Wartung der Sicherheit

Modul 19. Forensische Analyse

19.1. Datenerfassung und Replikation
- 19.1.1. Volatile Datenerfassung
  - 19.1.1.1. System-Informationen
  - 19.1.1.2. Netzwerk-Informationen
  - 19.1.1.3. Reihenfolge der Volatilität
- 19.1.2. Statische Datenerfassung
  - 19.1.2.1. Erstellung eines doppelten Bildes
  - 19.1.2.2. Erstellung eines Dokuments für die Überwachungskette
- 19.1.3. Methoden zur Validierung der erfassten Daten
  - 19.1.3.1. Methoden für Linux
  - 19.1.3.2. Methoden für Windows

19.2. Bewertung und Beseitigung von Anti-Forensik-Techniken
- 19.2.1. Ziele der forensischen Techniken
- 19.2.2. Löschung von Daten
  - 19.2.2.1. Löschung von Daten und Dateien
  - 19.2.2.2. Dateiwiederherstellung
  - 19.2.2.3. Wiederherstellung von gelöschten Partitionen
- 19.2.3. Passwortschutz
- 19.2.4. Steganographie
- 19.2.5. Sicheres Löschen von Geräten
- 19.2.6. Verschlüsselung

19.3. Betriebssystem-Forensik
- 19.3.1. Windows-Forensik
- 19.3.2. Linux-Forensik
- 19.3.3. Mac-Forensik

19.4. Netzwerk-Forensik
- 19.4.1. Log-Analyse
- 19.4.2. Korrelation der Daten
- 19.4.3. Netzwerk-Untersuchung
- 19.4.4. Schritte der forensischen Netzwerkanalyse

19.5. Web-Forensik
- 19.5.1. Untersuchung von Webangriffen
- 19.5.2. Angriffserkennung
- 19.5.3. Standort der IP-Adresse

19.6. Datenbank-Forensik
- 19.6.1. MSSQL-Forensik
- 19.6.2. MySQL-Forensik
- 19.6.3. PostgreSQL-Forensik
- 19.6.4. MongoDB-Forensik

19.7. *Cloud*-Forensik
- 19.7.1. Arten von *Cloud*-Verbrechen
  - 19.7.1.1. *Cloud* als Thema
  - 19.7.1.2. *Cloud* als Objekt
  - 19.7.1.3. *Cloud* als Werkzeug
- 19.7.2. Herausforderungen der *Cloud*-Forensik
- 19.7.3. Untersuchung von *Cloud*-Speicherdiensten
- 19.7.4. Forensische Analyse-Tools für die *Cloud*

19.8. Untersuchung von E-Mail-Verbrechen
- 19.8.1. Mail-Systeme
  - 19.8.1.1. *Mail Clients*
  - 19.8.1.2. Mail-Server
  - 19.8.1.3. SMTP-Server
  - 19.8.1.4. POP3-Server
  - 19.8.1.5. IMAP4-Server
- 19.8.2. Mail-Verbrechen
- 19.8.3. Mail-Nachricht
  - 19.8.3.1. Standard-Kopfzeilen
  - 19.8.3.2. Erweiterte Kopfzeilen
- 19.8.4. Schritte bei der Untersuchung dieser Verbrechen
- 19.8.5. Tools für die E-Mail-Forensik

19.9. Mobile forensische Analyse
- 19.9.1. Zellulare Netzwerke
  - 19.9.1.1. Arten von Netzwerken
  - 19.9.1.2. CDR-Inhalt
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Logische Akquisition
- 19.9.4. Physische Akquisition
- 19.9.5. Dateisystem-Erfassung

19.10. Forensische Berichte schreiben und einreichen
- 19.10.1. Wichtige Aspekte eines forensischen Berichts
- 19.10.2. Klassifizierung und Arten von Berichten
- 19.10.3. Leitfaden zum Schreiben eines Berichts
- 19.10.4. Präsentation des Berichts
  - 19.10.4.1. Vorbereitung auf die Zeugenaussage
  - 19.10.4.2. Hinterlegung
  - 19.10.4.3. Der Umgang mit den Medien

Modul 20. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

20.1. *Blockchain*-Technologie
- 20.1.1. Anwendungsbereiche
- 20.1.2. Garantie der Vertraulichkeit
- 20.1.3. Garantie der Nicht Abstreitbarkeit

20.2. Digitales Geld
- 20.2.1. Bitcoins
- 20.2.2. Kryptowährungen
- 20.2.3. Schürfen von Kryptowährungen
- 20.2.4. Schneeballsysteme
- 20.2.5. Andere mögliche Verbrechen und Probleme

20.3. *Deepfake*
- 20.3.1. Auswirkungen auf die Medien
- 20.3.2. Gefahren für die Gesellschaft
- 20.3.3. Erkennungsmechanismen

20.4. Die Zukunft der künstlichen Intelligenz
- 20.4.1. Künstliche Intelligenz und kognitives Computing
- 20.4.2. Anwendungen zur Vereinfachung des Kundendienstes

20.5. Digitale Privatsphäre
- 20.5.1. Wert der Daten im Netzwerk
- 20.5.2. Verwendung von Daten im Netzwerk
- 20.5.3. Datenschutz und Verwaltung digitaler Identitäten

20.6. Cyberkonflikte, Cyberkriminelle und Cyberangriffe
- 20.6.1. Auswirkungen der Cybersicherheit auf internationale Konflikte
- 20.6.2. Folgen von Cyberangriffen auf die allgemeine Bevölkerung
- 20.6.3. Arten von Cyberkriminellen. Schutzmaßnahmen

20.7. Telearbeit
- 20.7.1. Revolution der Telearbeit während und nach Covid19
- 20.7.2. Engpässe beim Zugang
- 20.7.3. Variation der Angriffsfläche
- 20.7.4. Bedürfnisse der Arbeiter

20.8. Aufkommende *Wireless*-Technologien
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Millimeter-Wellen
- 20.8.4. Trend zu *Get Smart* anstelle von *Get More*

20.9. Künftige Adressierung in Netzwerken
- 20.9.1. Aktuelle Probleme mit der IP-Adressierung
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. Vorteile von IPv4+ gegenüber IPv4
- 20.9.5. Vorteile von IPv6 gegenüber IPv4

20.10. Die Herausforderung, das Bewusstsein für eine frühzeitige und kontinuierliche Schulung der Bevölkerung zu schärfen
- 20.10.1. Aktuelle Strategien der Regierung
- 20.10.2. Der Widerstand der Menschen gegen das Lernen
- 20.10.3. Schulungspläne, die von den Unternehmen angenommen werden müssen

Sie werden anhand realer Fälle lernen, die in simulierten Lernumgebungen entwickelt wurden und die heutigen Herausforderungen im Bereich Datenmanagement und Cybersicherheit widerspiegeln“

04

Lehrziele

Das Hauptziel des Weiterbildenden Masterstudiengangs in Secure Information Management ist es, den Studenten hervorragende Kenntnisse in zwei grundlegenden und sich ergänzenden Bereichen der Informatik und des Ingenieurwesens zu vermitteln: Datenmanagement in digitalen Umgebungen und Cybersicherheit. Dieses Programm kombiniert beide Disziplinen, um Fachleute in der Umsetzung fortschrittlicher Lösungen fortzubilden, die es ihnen ermöglichen, die Herausforderungen ihrer Arbeit mit den notwendigen Werkzeugen zu bewältigen, um sensible Informationen in ihren Organisationen zu verwalten und zu schützen.

Verwandeln Sie Ihre Karriere mit diesem innovativen weiterbildenden Masterstudiengang, der ein Vorher und ein Nachher in Ihrer Spezialisierung auf Datenmanagement und Cybersicherheit markiert“

Allgemeine Ziele

- Entwickeln fortgeschrittener Fähigkeiten in den Bereichen Datenanalyse und Cybersicherheit um Geschäftsprozesse mit innovativen Tools und Techniken zu optimieren
- Implementieren wirksamer Sicherheitsstrategien zur Abwehr digitaler Bedrohungen für Systeme, Netzwerke und mobile Geräte
- Lösen von Cybersicherheitsherausforderungen durch Auditing, *Reverse Engineering* und evidenzbasierte Forensik
- Antizipieren von Technologietrends durch Anwendung bahnbrechender Lösungen zum Schutz digitaler Werte und fortschrittlicher Systeme

Führen Sie mit diesem Spezialisierungsprogramm das Datenmanagement und die Cybersicherheit in der digitalen Umgebung an“

Spezifische Ziele

Modul 1. Datenanalytik in der Unternehmensorganisation

- Entwickeln von Kompetenzen in der Anwendung von Datenanalysetechniken
- Erzeugen wertvoller Informationen, die die strategische Entscheidungsfindung in Unternehmen unterstützen und die Effizienz und Wettbewerbsfähigkeit verbessern

Modul 2. Management und Bearbeitung von Daten und Informationen für die Datenwissenschaft

- Fortbilden in der effizienten Verwaltung und Manipulation großer Datenmengen
- Anwenden von Methoden und Tools zur Strukturierung, Bereinigung und Umwandlung von Daten in nützliche Informationen für *Data-Science*-Projekte

Modul 3. IoT-Geräte und Plattformen als Grundlage für die Datenwissenschaft

- Vermitteln der notwendigen Kenntnisse über IoT-Plattformen und -Geräte und deren Integration in die Datenwissenschaft
- Vertiefen der Erfassung, Verarbeitung und Analyse von Echtzeitdaten

Modul 4. Grafische Darstellung für die Datenanalyse

- Grafisches Darstellen von Daten mit Hilfe fortschrittlicher Visualisierungstools und -techniken
- Erleichtern des Verständnisses von Mustern, Trends und Beziehungen in großen Datensätzen

Modul 5. Tools der Datenwissenschaft

- Fortbilden in der Verwendung spezifischer *Data-Science*-Tools und -Software, wie z. B. Python
- Vertiefen der Sammlung, Analyse und Präsentation von Daten in einer Vielzahl von beruflichen Kontexten

Modul 6. *Data Mining*. Auswahl, Vorverarbeitung und Transformation

- Vermitteln der Kenntnisse und Fähigkeiten, die für die Anwendung von *Data-Mining*-Techniken erforderlich sind
- Analysieren Sie die Auswahl, Vorverarbeitung und Umwandlung von Daten, um aussagekräftige Muster und Trends zu extrahieren

Modul 7. Vorhersagbarkeit und Analyse von stochastischen Phänomenen

- Entwickeln von Fähigkeiten zur Modellierung und Analyse stochastischer Phänomene
- Anwenden fortgeschrittener statistischer Methoden zur Vorhersage von Verhalten und Trends in unsicheren und dynamischen Umgebungen

Modul 8. Design und Entwicklung von intelligenten Systemen

- Fortbilden in der Konzeption und Entwicklung intelligenter Systeme unter Einbeziehung von Techniken des maschinellen Lernens und der künstlichen Intelligenz
- Erstellen von automatischen Lösungen, die komplexe Probleme effizient beheben

Modul 9. Datenintensive Architekturen und Systeme

- Vermitteln von Kenntnissen über die Schaffung von Systemarchitekturen, die große Datenmengen effizient verarbeiten können
- Verwenden fortschrittlicher Technologien wie verteilte Datenbanken und Parallelverarbeitung

Modul 10. Praktische Anwendung der Datenwissenschaft in Geschäftsbereichen

- Entwickeln der Fähigkeit, datenwissenschaftliche Praktiken in verschiedenen Geschäftsbereichen anzuwenden
- Integrieren des erworbenen Wissens zur Verbesserung der Entscheidungsfindung, Prozessoptimierung und Innovation im Unternehmen

Modul 11. Cyberintelligenz und Cybersicherheit

- Vermitteln der Kenntnisse und Fähigkeiten, die zur Anwendung von Cyberintelligenz- und Cybersicherheitstechniken erforderlich sind.
- Schützen von Unternehmenssystemen und -netzen vor Cyberbedrohungen und Sicherstellen der Datenintegrität

Modul 12. Host-Sicherheit

- Fortbilden in der Umsetzung von Sicherheitsmaßnahmen auf Hostsystemen
- Gewährleisten des Schutzes von Servern und kritischen Anwendungen durch den Einsatz von Tools und guten IT-Sicherheitspraktiken

Modul 13. Netzwerksicherheit (Perimeter)

- Vermitteln von Kenntnissen über den Schutz von Netzwerken und Computersystemen auf der Perimeterebene
- Verwalten von *Firewalls*, VPNs und anderen Tools zur Gewährleistung der Sicherheit in der Netzwerkinfrastruktur des Unternehmens

Modul 14. Smartphone-Sicherheit

- Entwickeln von Kompetenzen zur Gewährleistung der Sicherheit auf mobilen Geräten
- Verstehen gängiger Schwachstellen und Anwendung von Präventivmaßnahmen zum Schutz von Informationen und Anwendungen auf Smartphones

Modul 15. IoT-Sicherheit

- Vermitteln der notwendigen Kenntnisse zur Implementierung von Sicherheitslösungen für IoT-Geräte
- Schützen von Netzen und Systemen, die Geräte miteinander verbinden, und Garantieren der Vertraulichkeit und Integrität der erzeugten Daten

Modul 16. Ethisches *Hacking*

- Fortbilden in ethischen Hacking-Praktiken, wobei die Durchführung von kontrollierten Penetrationstests gelehrt wird
- Identifizieren von Schwachstellen in Computersystemen zur Verbesserung der Sicherheit, bevor sie von Angreifern ausgenutzt werden können

Modul 17. *Reverse Engineering*

- Vermitteln von Kenntnissen über Reverse-Engineering-Techniken, die die Analyse und das Verständnis der Funktionsweise von Software und Hardware ermöglichen
- Aufdecken von Sicherheitslücken oder Verbesserung der Funktionalität bestehender Systeme

Modul 18. Sichere Entwicklung

- Vermitteln guter Programmier- und Sicherheitspraktiken während des Software-Lebenszyklus
- In der Lage sein, Schwachstellen zu vermeiden und Computersysteme vor Angriffen zu schützen

Modul 19. Forensische Analyse

- Entwickeln der erforderlichen Fähigkeiten zur Durchführung digitaler forensischer Untersuchungen
- Verwenden fortgeschrittener Werkzeuge und Techniken zur Wiederherstellung, Analyse und Sicherung elektronischer Beweise bei Computersicherheitsvorfällen

Modul 20. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

- Untersuchen aktueller und zukünftiger Herausforderungen im Bereich der Computersicherheit, Analysieren neuer Bedrohungen und neuer Schutztechnologien
- Vertiefen der Strategien zur Risikominderung in einem sich ständig verändernden technologischen Umfeld

05

Karrieremöglichkeiten

Nach Abschluss dieses Weiterbildenden Masterstudiengangs in Secure Information Management werden Fachleute ein solides Verständnis für die fortschrittlichsten Strategien im Bereich der Cybersicherheit und des digitalen Datenmanagements erworben haben. Die Absolventen werden darauf vorbereitet, Lösungen zu entwerfen und zu implementieren, die den Schutz sensibler Informationen gewährleisten und die Analyse- und Entscheidungsprozesse in Geschäftsumgebungen optimieren. Auf diese Weise verbessern sie ihre Berufsaussichten und übernehmen spezialisierte Aufgaben als Cybersicherheitsanalytiker, Geheimdienstberater oder Manager für kritische Daten.

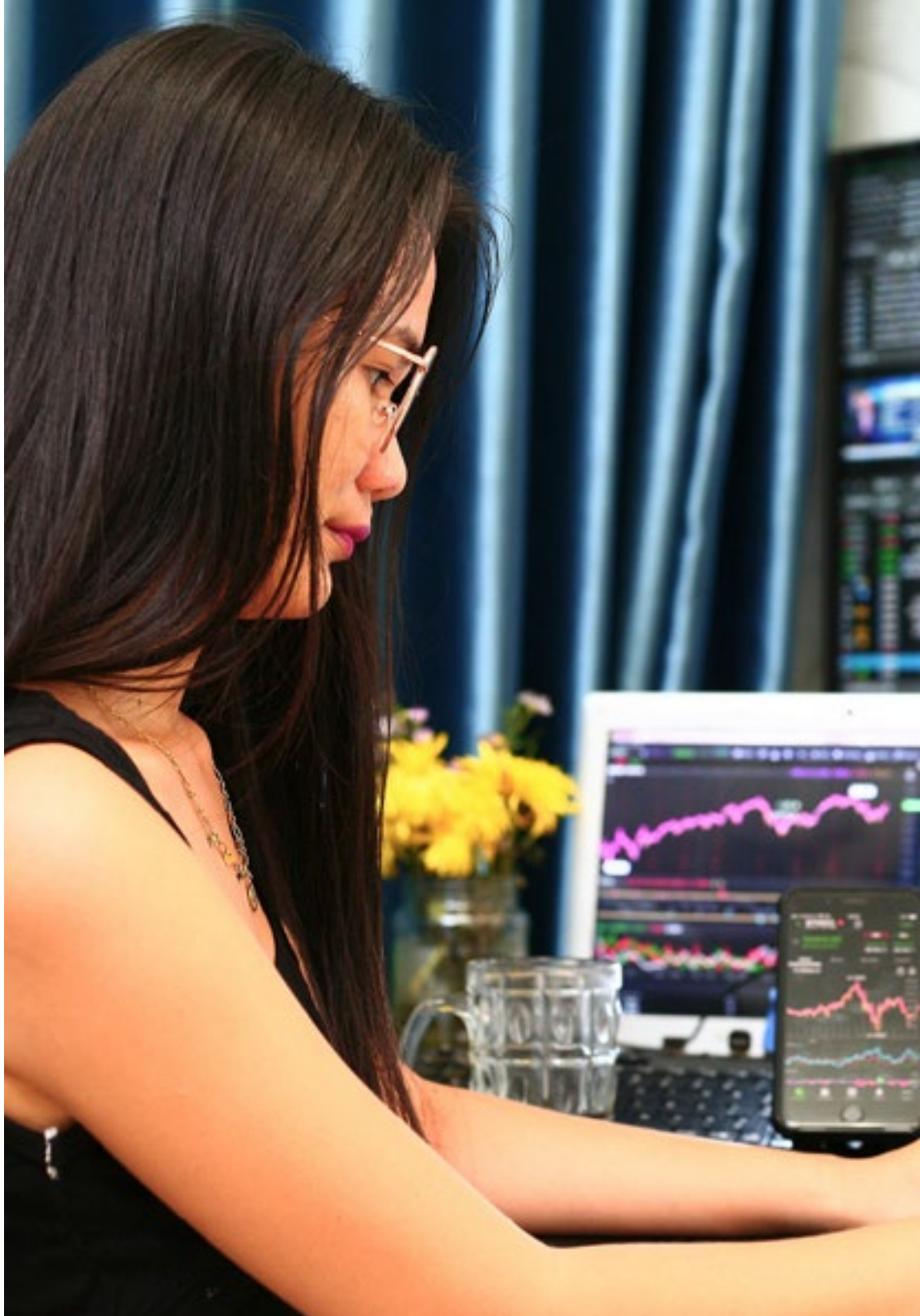
Sie werden für die Sicherheit digitaler Güter sorgen und eine Schlüsselrolle bei der digitalen Transformation von Unternehmen spielen“

Profil des Absolventen

Der Absolvent des Weiterbildenden Masterstudiengangs in Secure Information Management wird bestens fortgebildet sein, um Informationen in digitalen Umgebungen zu verwalten und zu schützen. Er wird über fortgeschrittene Kenntnisse in Bereichen wie Cybersicherheit, digitale Intelligenz und Datenanalyse sowie über praktische Fähigkeiten bei der Konzeption und Umsetzung von Strategien zur Abwehr von Bedrohungen verfügen. Sein Profil verbindet ein tiefes technisches Verständnis mit strategischen Kompetenzen, die es ihm ermöglichen, Projekte in wichtigen Geschäftsbereichen zu leiten.

Sie werden eine führende Position im Bereich Datenschutz und Cybersicherheit einnehmen und mit Unternehmen zusammenarbeiten, um die Herausforderungen des digitalen Umfelds zu meistern.

- **Sicherheitsmanagement:** Entwicklung der Fähigkeit, Risiken zu erkennen, mehrschichtige Verteidigungsstrategien umzusetzen und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten
- **Kritisches Analyse und Problemlösung:** Sie werden erweiterte Techniken anwenden, um Systeme zu bewerten, Schwachstellen zu erkennen und Lösungen zu entwerfen, die an unterschiedliche technologische Umgebungen angepasst sind
- **Technische und digitale Kompetenz:** Sie werden mit fortgeschrittenen Werkzeugen für die Datenanalyse, die Cybersicherheit und nachrichtendienstliche Systeme umgehen und in der Lage sein, Projekte zur technologischen Innovation zu leiten
- **Strategisches Denken:** Sie werden Sicherheits- und Geschäftsstrategien entwerfen, die den aktuellen und künftigen Anforderungen des digitalen Umfelds gerecht werden
- **Interdisziplinäre Zusammenarbeit:** Sie werden mit multidisziplinären Teams zusammenarbeiten, um komplexe Herausforderungen zu bewältigen und die Sicherheit von Netzwerken, IoT-Plattformen und mobilen Geräten zu gewährleisten



Nach Abschluss des weiterbildenden Masterstudiengangs werden Sie in der Lage sein, Ihre Kenntnisse und Fähigkeiten in den folgenden Positionen anzuwenden:

1. **Direktor für Cybersicherheit:** Führungskraft, die für die Koordinierung von Teams und die Entwicklung von Strategien zum Schutz digitaler Ressourcen in großen Organisationen zuständig ist.
2. **Datenanalyst:** Entwickler von prädiktiven Analyse- und Visualisierungssystemen zur Optimierung der Entscheidungsfindung.
3. **Berater für digitale Intelligenz:** Berater, der darauf spezialisiert ist, fortschrittliche Lösungen auf der Grundlage von Intelligenz und Risikoanalyse anzubieten.
4. **IoT- und Sicherheitsspezialist:** Entwickler von Schutzmaßnahmen für vernetzte Geräte und industrielle Umgebungen.
5. **Ethischer Hacker:** Schwachstellenprüfer, der Schwachstellen in Unternehmenssystemen behebt, um Cyberangriffe zu verhindern
6. **Sicherheitsauditor:** Prüfer, der Audits und forensische Analysen durchführt, um die Einhaltung von Vorschriften zu gewährleisten
7. **Verwalter von Unternehmensdaten:** Verwalter, der für die Entwicklung und Verwaltung von Speicher- und Analysesystemen zur Verbesserung der betrieblichen Effizienz zuständig ist.

Absolvieren Sie dieses Programm und profilieren Sie sich als Spezialist in den gefragtesten Bereichen des digitalen Umfelds“

06

Studienmethodik

TECH ist die erste Universität der Welt, die die Methodik der ***case studies*** mit ***Relearning*** kombiniert, einem 100%igen Online-Lernsystem, das auf geführten Wiederholungen basiert.

Diese disruptive pädagogische Strategie wurde entwickelt, um Fachleuten die Möglichkeit zu bieten, ihr Wissen zu aktualisieren und ihre Fähigkeiten auf intensive und gründliche Weise zu entwickeln. Ein Lernmodell, das den Studenten in den Mittelpunkt des akademischen Prozesses stellt und ihm die Hauptrolle zuweist, indem es sich an seine Bedürfnisse anpasst und die herkömmlichen Methoden beiseite lässt.

TECH bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein“

Der Student: die Priorität aller Programme von TECH

Bei der Studienmethodik von TECH steht der Student im Mittelpunkt.
Die pädagogischen Instrumente jedes Programms wurden unter Berücksichtigung der Anforderungen an Zeit, Verfügbarkeit und akademische Genauigkeit ausgewählt, die heutzutage nicht nur von den Studenten, sondern auch von den am stärksten umkämpften Stellen auf dem Markt verlangt werden.

Beim asynchronen Bildungsmodell von TECH entscheidet der Student selbst, wie viel Zeit er mit dem Lernen verbringt und wie er seinen Tagesablauf gestaltet, und das alles bequem von einem elektronischen Gerät seiner Wahl aus. Der Student muss nicht an Präsenzveranstaltungen teilnehmen, die er oft nicht wahrnehmen kann.
Die Lernaktivitäten werden nach eigenem Ermessen durchgeführt. Er kann jederzeit entscheiden, wann und von wo aus er lernen möchte.

Bei TECH gibt es KEINE Präsenzveranstaltungen (an denen man nie teilnehmen kann)“

Die international umfassendsten Lehrpläne

TECH zeichnet sich dadurch aus, dass sie die umfassendsten Studiengänge im universitären Umfeld anbietet. Dieser Umfang wird durch die Erstellung von Lehrplänen erreicht, die nicht nur die wesentlichen Kenntnisse, sondern auch die neuesten Innovationen in jedem Bereich abdecken.

Durch ihre ständige Aktualisierung ermöglichen diese Programme den Studenten, mit den Veränderungen des Marktes Schritt zu halten und die von den Arbeitgebern am meisten geschätzten Fähigkeiten zu erwerben. Auf diese Weise erhalten die Studenten, die ihr Studium bei TECH absolvieren, eine umfassende Vorbereitung, die ihnen einen bedeutenden Wettbewerbsvorteil verschafft, um in ihrer beruflichen Laufbahn voranzukommen.

Und das von jedem Gerät aus, ob PC, Tablet oder Smartphone.

> *Das Modell der TECH ist asynchron, d. h. Sie können an Ihrem PC, Tablet oder Smartphone studieren, wo immer Sie wollen, wann immer Sie wollen und so lange Sie wollen“*

Case studies oder Fallmethode

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Wirtschaftshochschulen der Welt. Sie wurde 1912 entwickelt, damit Studenten der Rechtswissenschaften das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernten, sondern auch mit realen komplexen Situationen konfrontiert wurden. Auf diese Weise konnten sie fundierte Entscheidungen treffen und Werturteile darüber fällen, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

Bei diesem Lehrmodell ist es der Student selbst, der durch Strategien wie *Learning by doing* oder *Design Thinking*, die von anderen renommierten Einrichtungen wie Yale oder Stanford angewandt werden, seine berufliche Kompetenz aufbaut.

Diese handlungsorientierte Methode wird während des gesamten Studiengangs angewandt, den der Student bei TECH absolviert. Auf diese Weise wird er mit zahlreichen realen Situationen konfrontiert und muss Wissen integrieren, recherchieren, argumentieren und seine Ideen und Entscheidungen verteidigen. All dies unter der Prämisse, eine Antwort auf die Frage zu finden, wie er sich verhalten würde, wenn er in seiner täglichen Arbeit mit spezifischen, komplexen Ereignissen konfrontiert würde.

Relearning-Methode

Bei TECH werden die *case studies* mit der besten 100%igen Online-Lernmethode ergänzt: *Relearning*.

Diese Methode bricht mit traditionellen Lehrmethoden, um den Studenten in den Mittelpunkt zu stellen und ihm die besten Inhalte in verschiedenen Formaten zu vermitteln. Auf diese Weise kann er die wichtigsten Konzepte der einzelnen Fächer wiederholen und lernen, sie in einem realen Umfeld anzuwenden.

In diesem Sinne und gemäß zahlreicher wissenschaftlicher Untersuchungen ist die Wiederholung der beste Weg, um zu lernen. Aus diesem Grund bietet TECH zwischen 8 und 16 Wiederholungen jedes zentralen Konzepts innerhalb ein und derselben Lektion, die auf unterschiedliche Weise präsentiert werden, um sicherzustellen, dass das Wissen während des Lernprozesses vollständig gefestigt wird.

Das Relearning ermöglicht es Ihnen, mit weniger Aufwand und mehr Leistung zu lernen, sich mehr auf Ihre Spezialisierung einzulassen, einen kritischen Geist zu entwickeln, Argumente zu verteidigen und Meinungen zu kontrastieren: eine direkte Gleichung zum Erfolg.

Ein 100%iger virtueller Online-Campus mit den besten didaktischen Ressourcen

Um seine Methodik wirksam anzuwenden, konzentriert sich TECH darauf, den Studenten Lehrmaterial in verschiedenen Formaten zur Verfügung zu stellen: Texte, interaktive Videos, Illustrationen und Wissenskarten, um nur einige zu nennen. Sie alle werden von qualifizierten Lehrkräften entwickelt, die ihre Arbeit darauf ausrichten, reale Fälle mit der Lösung komplexer Situationen durch Simulationen, dem Studium von Zusammenhängen, die für jede berufliche Laufbahn gelten, und dem Lernen durch Wiederholung mittels Audios, Präsentationen, Animationen, Bildern usw. zu verbinden.

Die neuesten wissenschaftlichen Erkenntnisse auf dem Gebiet der Neurowissenschaften weisen darauf hin, dass es wichtig ist, den Ort und den Kontext, in dem der Inhalt abgerufen wird, zu berücksichtigen, bevor ein neuer Lernprozess beginnt. Die Möglichkeit, diese Variablen individuell anzupassen, hilft den Menschen, sich zu erinnern und Wissen im Hippocampus zu speichern, um es langfristig zu behalten. Dies ist ein Modell, das als *Neurocognitive context-dependent e-learning* bezeichnet wird und in diesem Hochschulstudium bewusst angewendet wird.

Zum anderen, auch um den Kontakt zwischen Mentor und Student so weit wie möglich zu begünstigen, wird eine breite Palette von Kommunikationsmöglichkeiten angeboten, sowohl in Echtzeit als auch zeitversetzt (internes Messaging, Diskussionsforen, Telefondienst, E-Mail-Kontakt mit dem technischen Sekretariat, Chat und Videokonferenzen).

Darüber hinaus wird dieser sehr vollständige virtuelle Campus den Studenten der TECH die Möglichkeit geben, ihre Studienzeiten entsprechend ihrer persönlichen Verfügbarkeit oder ihren beruflichen Verpflichtungen zu organisieren. Auf diese Weise haben sie eine globale Kontrolle über die akademischen Inhalte und ihre didaktischen Hilfsmittel, in Übereinstimmung mit ihrer beschleunigten beruflichen Weiterbildung.

> *Der Online-Studienmodus dieses Programms wird es Ihnen ermöglichen, Ihre Zeit und Ihr Lerntempo zu organisieren und an Ihren Zeitplan anzupassen“*

Die Wirksamkeit der Methode wird durch vier Schlüsselergebnisse belegt:

1. Studenten, die diese Methode anwenden, nehmen nicht nur Konzepte auf, sondern entwickeln auch ihre geistigen Fähigkeiten durch Übungen zur Bewertung realer Situationen und zur Anwendung ihres Wissens.
2. Das Lernen basiert auf praktischen Fähigkeiten, die es den Studenten ermöglichen, sich besser in die reale Welt zu integrieren.
3. Eine einfachere und effizientere Aufnahme von Ideen und Konzepten wird durch die Verwendung von Situationen erreicht, die aus der Realität entstanden sind.
4. Das Gefühl der Effizienz der investierten Anstrengung wird zu einem sehr wichtigen Anreiz für die Studenten, was sich in einem größeren Interesse am Lernen und einer Steigerung der Zeit, die für die Arbeit am Kurs aufgewendet wird, niederschlägt.

Die von ihren Studenten am besten bewertete Hochschulmethodik

Die Ergebnisse dieses innovativen akademischen Modells lassen sich an der Gesamtzufriedenheit der Absolventen der TECH ablesen.

Die Studenten bewerten die Qualität der Lehre, die Qualität der Materialien, die Kursstruktur und die Ziele als hervorragend. So überrascht es nicht, dass die Einrichtung von ihren Studenten auf der Bewertungsplattform Trustpilot mit 4,9 von 5 Punkten am besten bewertet wurde.

Sie können von jedem Gerät mit Internetanschluss (Computer, Tablet, Smartphone) auf die Studieninhalte zugreifen, da TECH in Sachen Technologie und Pädagogik führend ist.

Sie werden die Vorteile des Zugangs zu simulierten Lernumgebungen und des Lernens durch Beobachtung, d. h. Learning from an expert, nutzen können.

In diesem Programm stehen Ihnen die besten Lehrmaterialien zur Verfügung, die sorgfältig vorbereitet wurden:

Studienmaterial

Alle didaktischen Inhalte werden von den Fachkräfte, die den Kurs unterrichten werden, speziell für den Kurs erstellt, so dass die didaktische Entwicklung wirklich spezifisch und konkret ist.

Diese Inhalte werden dann auf ein audiovisuelles Format übertragen, das unsere Online-Arbeitsweise mit den neuesten Techniken ermöglicht, die es uns erlauben, Ihnen eine hohe Qualität in jedem der Stücke zu bieten, die wir Ihnen zur Verfügung stellen werden.

Übungen für Fertigkeiten und Kompetenzen

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein Spezialist im Rahmen der Globalisierung, in der wir leben, entwickeln muss.

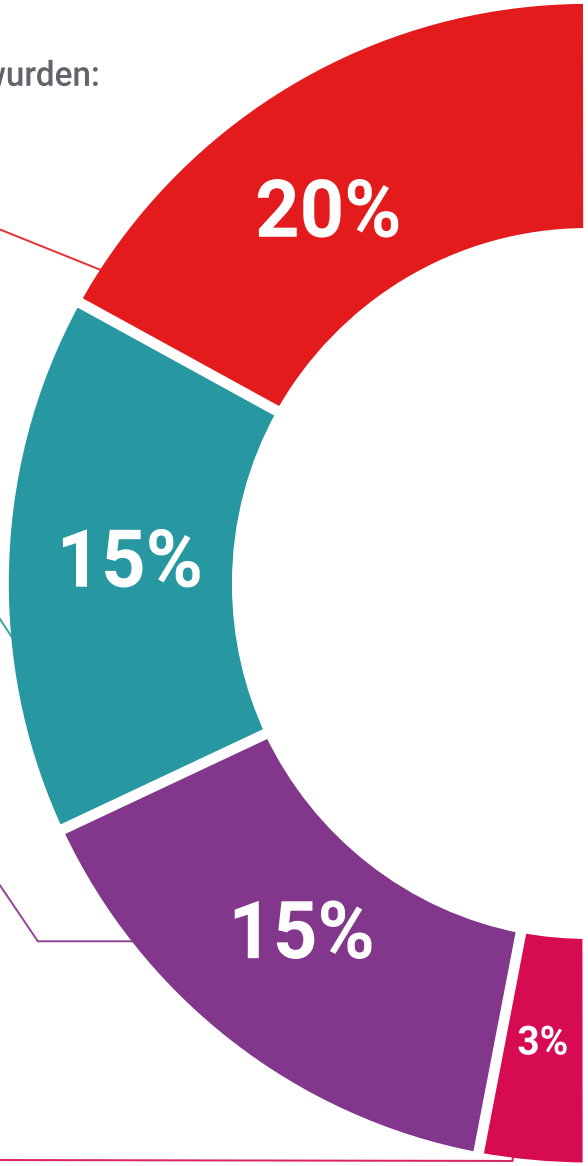
Interaktive Zusammenfassungen

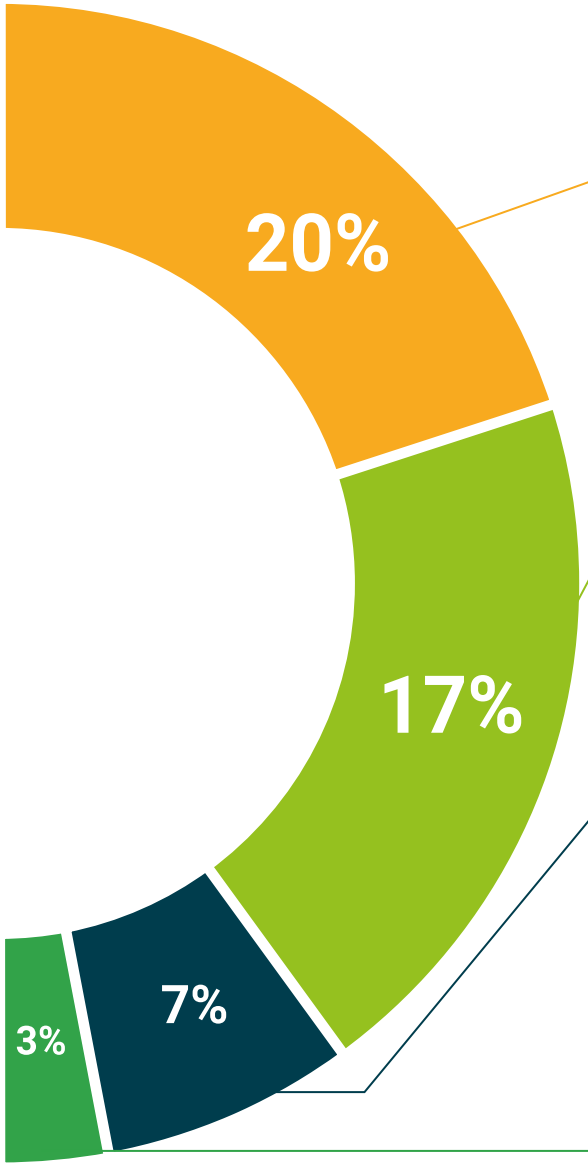
Wir präsentieren die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu festigen.

Dieses einzigartige System für die Präsentation multimedialer Inhalte wurde von Microsoft als „Europäische Erfolgsgeschichte" ausgezeichnet.

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente, internationale Leitfäden... In unserer virtuellen Bibliothek haben Sie Zugang zu allem, was Sie für Ihre Ausbildung benötigen.





Case Studies

Sie werden eine Auswahl der besten *case studies* zu diesem Thema bearbeiten. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.

Testing & Retesting

Während des gesamten Programms werden Ihre Kenntnisse in regelmäßigen Abständen getestet und wiederholt. Wir tun dies auf 3 der 4 Ebenen der Millerschen Pyramide.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

Das sogenannte *Learning from an Expert* stärkt das Wissen und das Gedächtnis und schafft Vertrauen in unsere zukünftigen schwierigen Entscheidungen.

Kurzanleitungen zum Vorgehen

TECH bietet die wichtigsten Inhalte des Kurses in Form von Arbeitsblättern oder Kurzanleitungen an. Ein synthetischer, praktischer und effektiver Weg, um dem Studenten zu helfen, in seinem Lernen voranzukommen.

07

Lehrkörper

Dieser Abschluss wird von führenden Fachleuten für Cybersicherheit und digitales Datenmanagement gelehrt. Ihre Erfahrung stellt sicher, dass die Studenten vollständige und aktuelle Inhalte erhalten, die direkt auf ihre berufliche Laufbahn anwendbar sind. So geben die Dozenten dieses Weiterbildenden Masterstudiengangs in Secure Information Management ihr Wissen weiter und bilden hochqualifizierte Spezialisten aus, die von großen internationalen Unternehmen nachgefragt werden.

Erwerben Sie mit den Besten das Wissen und die Schlüsselkompetenzen, um in den Bereichen Datenmanagement und Cybersicherheit im digitalen Umfeld führend zu sein“

Internationaler Gastdirektor

Dr. Frederic Lemieux ist international als innovativer Experte und inspirierende Führungspersönlichkeit in den Bereichen der **Intelligenz, der nationalen Sicherheit, der inneren Sicherheit, der Cybersicherheit** und der **disruptiven Technologien anerkannt.** Sein ständiges Engagement und seine wichtigen Beiträge zu Forschung und Bildung machen ihn zu einer zentralen Figur bei der Förderung der Sicherheit und des Verständnisses der heutigen neuen Technologien. Während seiner beruflichen Laufbahn hat er an mehreren renommierten Institutionen wie der **Universität von Montreal**, der **George Washington Universität** und der **Universität von Georgetown** zukunftsweisende akademische Programme konzipiert und geleitet.

Im Laufe seiner umfangreichen Erfahrung hat er mehrere Bücher von großer Bedeutung veröffentlicht, die sich alle mit **kriminalistischer Aufklärung, Polizeiarbeit, Cyber-Bedrohungen und internationaler Sicherheit** befassen. Er hat auch einen wichtigen Beitrag zum Bereich der Cybersicherheit geleistet, indem er zahlreiche Artikel in akademischen Zeitschriften veröffentlicht hat, die sich mit der Verbrechensbekämpfung bei großen Katastrophen, der Terrorismusbekämpfung, den Nachrichtendiensten und der polizeilichen Zusammenarbeit beschäftigen. Darüber hinaus war er Podiumsteilnehmer und Hauptredner bei verschiedenen nationalen und internationalen Konferenzen und hat sich als führender Wissenschaftler und Praktiker etabliert.

Dr. Lemieux hatte redaktionelle und bewertende Funktionen in verschiedenen akademischen, privaten und staatlichen Organisationen inne, was seinen Einfluss und sein Engagement für Spitzenleistungen in seinem Fachgebiet widerspiegelt. Im Rahmen seiner angesehenen akademischen Laufbahn war er Professor für Praktika und Leiter des Lehrkörpers der MPS-Programme für **Angewandte Intelligenz, Risikomanagement für Cybersicherheit, Technologiemanagement und Informationstechnologiemanagement** an der **Universität von Georgetown**.

Dr. Lemieux, Frederic

- Direktor des Masterstudiengangs in Cybersecurity Risk Management an der Georgetown University
- Direktor des Masterstudiengangs in Technology Management an der Georgetown University
- Direktor des Masterstudiengangs in Applied Intelligence an der Georgetown University
- Professor für Praktika an der Georgetown University
- Promotion in Kriminologie an der School of Criminology der Universität von Montreal
- Hochschulabschluss in Soziologie und Nebenfach Psychologie an der Universität Laval
- Mitglied von: New Program Roundtable Committee, Georgetown University

Dank TECH werden Sie mit den besten Fachleuten der Welt lernen können"

Leitung

Dr. Peralta Martín-Palomino, Arturo

- CEO und CTO bei Prometeus Global Solutions
- CTO bei Korporate Technologies
- CTO bei AI Shepherds GmbH
- Berater und strategischer Unternehmensberater bei Alliance Medical
- Direktor für Design und Entwicklung bei DocPath
- Promotion in Computertechnik an der Universität von Castilla La Mancha
- Promotion in Wirtschaftswissenschaften, Unternehmen und Finanzen an der Universität Camilo José Cela
- Promotion in Psychologie an der Universität von Castilla La Mancha
- Masterstudiengang Executive MBA von der Universität Isabel I
- Masterstudiengang in Business und Marketing Management von der Universität Isabel I
- Masterstudiengang in Big Data bei Formación Hadoop
- Masterstudiengang in Fortgeschrittene Informationstechnologie an der Universität von Castilla La Mancha
- Mitglied der SMILE-Forschungsgruppe

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical Hacking am Nationalen Referenzzentrum von Getafe für Informatik und Telekommunikation von Madrid
- Zertifizierte E-Council-Ausbilderin
- Ausbilderin für die folgenden Zertifizierungen: EXIN Ethical Hacking Foundation und EXIN Cyber & IT Security Foundation, Madrid
- Von der CAM akkreditierte Fachausbilderin für die folgenden Berufszertifikate: IT-Sicherheit (IFCT0190), Verwaltung von Sprach- und Datennetzen (IFCM0310), Verwaltung von Abteilungsnetzen (IFCT0410), Alarmmanagement in Telekommunikationsnetzen (IFCM0410), Betreiber von Sprach- und Datennetzen (IFCM0110) und Verwaltung von Internetdiensten (IFCT0509)
- Externe Mitarbeit CSO/SSA (*Chief Security Officer/Senior Security Architect*) an der Universität der Balearischen Inseln
- Computer-Ingenieurin von der Universität von Alcalá de Henares in Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training
- Microsoft Azure Security Techonologies, E-Council

Professoren

Hr. Montoro Montarroso, Andrés

- Forscher in der SMILe-Gruppe an der Universität von Castilla La Mancha
- Forscher an der Universität von Granada
- Datenwissenschaftler bei Prometeus Global Solutions
- Vizepräsident und Softwareentwickler bei CireBits
- Promotion in fortgeschrittener Informationstechnologie an der Universität von Castilla La Mancha
- Hochschulabschluss in Computertechnik an der Universität von Castilla La Mancha
- Masterstudiengang in Datenwissenschaft und Computertechnik an der Universität von Granada
- Gastprofessor für das Fach Wissensbasierte Systeme an der Hochschule für Informatik in Ciudad Real, der die Vorlesung hält: *Fortgeschrittene Techniken der künstlichen Intelligenz: Suche und Analyse potenzieller Radikaler in den sozialen Medien*
- Gastprofessor für das Fach Data Mining an der Hochschule für Informatik in Ciudad Real, der die Vorlesung hält: *Anwendungen der Verarbeitung natürlicher Sprache: Fuzzy Logic zur Analyse von Nachrichten in sozialen Netzwerken*
- Referent beim Seminar über Korruptionsprävention in der öffentlichen Verwaltung und künstliche Intelligenz an der Fakultät für Rechts- und Sozialwissenschaften von Toledo, der den Vortrag hält: *Techniken der künstlichen Intelligenz*
- Referent auf dem ersten internationalen Seminar über Verwaltungsrecht und künstliche Intelligenz (DAIA). Organisiert von dem Europäischen Studienzentrum Luis Ortega Álvarez und dem Forschungsinstitut TransJus. Konferenz mit dem Titel *Analyse von Gefühlen zur Verhinderung von Hassreden in sozialen Medien*

Hr. Peris Morillo, Luis Javier

- Senior Technical Lead und Delivery Lead Support bei HCL Technologies
- Technischer Redakteur bei Baeldung
- Agile Coach und Operations Manager bei Mirai Advisory
- Entwickler, Team Lead, Scrum Master, Agile Coach und Produktmanager bei DocPath
- Technologe bei ARCO
- Hochschulabschluss in Informatik-Ingenieurwesen an der Universität von Castilla La Mancha
- Aufbaustudiengang in Projektmanagement von CEOE

Fr. Fernández Meléndez, Galina

- Spezialistin für Big Data
- Datenanalystin bei Aresi Gestión de Fincas
- Datenanalystin bei ADN Mobile Solution
- Hochschulabschluss in Betriebswirtschaftslehre an der Universität Bicentenaria de Aragua, Caracas, Venezuela
- Universitätskurs in Planung und öffentlichen Finanzen von der venezolanischen Schule für Planung
- Masterstudiengang in Datenanalyse und Business Intelligence an der Universität von Oviedo
- MBA in Betriebswirtschaft und Management von der Europäischen Wirtschaftsschule von Barcelona
- Masterstudiengang in Big Data und Business Intelligence an der Europäischen Wirtschaftsschule von Barcelona

Fr. Pedrajas Parabás, María Elena

- New Technologies and Digital Transformation Consultant bei Management Solutions
- Forscherin in der Abteilung für Informatik und numerische Analyse an der Universität von Cordoba
- Forscherin am Singulären Zentrum für Forschung in intelligenten Technologien in Santiago de Compostela
- Hochschulabschluss in Computertechnik von der Universität von Córdoba
- Masterstudiengang in Datenwissenschaft und Computertechnik an der Universität von Granada
- Masterstudiengang in Unternehmensberatung an der Päpstlichen Universität Comillas

Fr. Martínez Cerrato, Yésica

- Leitung der technischen Fortbildung bei Securitas Seguridad España
- Expertin für Bildung, Wirtschaft und Marketing
- *Product Manager* für elektronische Sicherheit bei Securitas Seguridad España
- Business-Intelligence-Analyst bei Ricopia Technologies
- IT-Technikerin - Verantwortlich für die OTEC-Computerräume an der Universität von Alcalá de Henares
- Mitwirkung in der Vereinigung ASALUMA
- Hochschulabschluss in Elektronischer Kommunikationstechnik an der Polytechnischen Hochschule der Universität von Alcalá

Hr. Fondón Alcalde, Rubén

- Analyst EMEA bei Amazon Web Services
- Business Analyst im Bereich Kundenwertmanagement bei Vodafone Spanien
- Leitung der Abteilung Service Integration bei Entelgy für Telefónica Global Solutions
- Online-Kundenbetreuung für Klon-Server bei EDM Electronics
- Implementierungsmanager für internationale Dienste bei Vodafone Global Enterprise
- Lösungsberater für Spanien und Portugal bei Telvent Global Services
- Business Analyst für Südeuropa bei Vodafone Global Enterprise
- Ingenieur für Telekommunikation von der Europäischen Universität von Madrid
- Masterstudiengang in Big Data und Analytics an der Internationalen Universität von Valencia

Hr. Díaz Díaz-Chirón, Tobías

- Forscher im ArCO-Labor der Universität von Castilla La Mancha
- Berater bei Blue Telecom
- Freiberufler, der sich hauptsächlich mit dem Telekommunikationssektor beschäftigt und sich auf 4G/5G-Netze spezialisiert hat
- OpenStack: deploy and administration
- Hochschulabschluss in Senior IT-Techniker an der Universität von Castilla La Mancha
- Spezialisierung auf Computerarchitektur und Netzwerke
- Außerordentlicher Professor an der Universität von Castilla La Mancha
- Referent beim Sepecam-Kurs über Netzwerkverwaltung

Hr. Tato Sánchez, Rafael

- Technischer Direktor bei Indra Sistemas SA
- Systemingenieur bei ENA Tráfico SAU
- Masterstudiengang in Industrie 4.0 von der Online-Universität
- Masterstudiengang in Wirtschaftsingenieurwesen von der Europäischen Universität
- Hochschulabschluss Industrie- und Automatisierungselektronik von der Europäischen Universität
- Wirtschaftsingenieur von der Polytechnischen Universität von Madrid

Fr. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applikationsentwicklung bei B60, UK
- Analytikerin-Programmiererin für die Verwaltung, Koordination und Dokumentation einer virtualisierten Sicherheitsalarmumgebung
- Analytikerin-Programmiererin von Java-Anwendungen in Geldautomaten für Kunden
- *Software-Development*-Expertin für die Validierung von Unterschriften und die Anwendung zur Dokumentenverwaltung
- Systemtechnikerin für die Migration von Geräten und für die Verwaltung, Wartung und Schulung von PDA-Mobilgeräten vor Ort
- Technische Ingenieurin für Computersysteme von der Offenen Universität von Katalonien (UOC)
- Masterstudiengang in Computersicherheit und Ethical Hacking von Offizieller EC-Council und CompTIA an der Fachhochschule für neue Technologien CICE

Hr. Catalá Barba, José Francisco

- Elektroniker mit Erfahrung in Cybersicherheit
- Entwickler von mobilen Anwendungen
- Elektroniker im mittleren Führungsstab des spanischen Verteidigungsministeriums
- Elektroniker im Ford-Werk in Valencia

Hr. Armero Fernández, Rafael

- Business Intelligence Consultant bei SDG Group
- Digital Engineer bei MI-GSO
- Logistic Engineer bei Torrecid SA
- Quality Intern bei INDRA
- Hochschulabschluss in Luft- und Raumfahrttechnik an der Polytechnischen Universität von Valencia
- Masterstudiengang in Professional Development 4.0 an der Universität von Alcalá

Hr. Peralta Alonso, Jon

- Senior Consultant - Datenschutz und Cybersicherheit
- Jurist / Rechtsberater bei Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Rechtsberater / Praktikant in einer professionellen Kanzlei: Óscar Padura
- Hochschulabschluss in Jura an der Öffentlichen Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter an der EIS Innovative School
- Masterstudiengang in Anwaltschaft an der Öffentlichen Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht an der Internationalen Universität Isabel I de Castilla
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht

Hr. Redondo, Jesús Serrano

- Webentwickler und Cybersecurity-Techniker
- Web-Entwickler bei Roams, Palencia
- FrontEnd-Entwickler bei Telefónica, Madrid
- FrontEnd-Entwickler bei Best Pro Consulting SL, Madrid
- Installateur für Telekommunikationseinrichtungen und -dienste bei Grupo Zener, Castilla und León
- Installateur für Telekommunikationsanlagen und -dienste bei Lican Comunicaciones SL, Castilla y León
- Zertifikat in Computersicherheit, CFTIC Getafe, Madrid
- Höhere Berufsausbildung in Telekommunikations- und Computersysteme vom IES Trinidad Arroyo, Palencia
- Höhere Berufsausbildung in elektrotechnischen Installationen für Mittel- und Niederspannungsnetze vom IES Trinidad Arroyo, Palencia
- Fortbildung in Reverse Engineering, Stenografie und Verschlüsselung an der Incibe Hacker Academy

Hr. Jiménez Ramos, Álvaro

- Cybersecurity Analyst
- Senior Sicherheitsanalyst bei The Workshop
- L1 Cybersecurity Analyst bei Axians
- L2 Cybersecurity Analyst bei Axians
- Cybersecurity Analyst bei SACYR S.A.
- Hochschulabschluss in Telematik-Ingenieurwesen an der Polytechnischen Universität von Madrid
- Masterstudiengang in Cybersicherheit und ethisches Hacken von CICE
- Fortgeschrittenenkurs in Cybersicherheit von Deusto Formación

Nutzen Sie die Gelegenheit, sich über die neuesten Fortschritte auf diesem Gebiet zu informieren und diese in Ihrer täglichen Praxis anzuwenden"

08
Qualifizierung

Der Weiterbildender Masterstudiengang in Secure Information Management garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.

Schließen Sie dieses Programm erfolgreich ab und erhalten Sie Ihren Universitätsabschluss ohne lästige Reisen oder Formalitäten"

Dieser **Weiterbildender Masterstudiengang in Secure Information Management** enthält das vollständigste und aktuellste Programm auf dem Markt.

Sobald der Student die Prüfungen bestanden hat, erhält er/sie per Post* mit Empfangsbestätigung das entsprechende Diplom, ausgestellt von der **TECH Technologischen Universität.**

Das von **TECH Technologische Universität** ausgestellte Diplom drückt die erworbene Qualifikation aus und entspricht den Anforderungen, die in der Regel von Stellenbörsen, Auswahlprüfungen und Berufsbildungsausschüssen verlangt werden.

Titel: **Weiterbildender Masterstudiengang in Secure Information Management**

Modalität: **online**

Dauer: **2 Jahre**

tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

WEITERBILDENDER MASTERSTUDIENGANG

in

Secure Information Management

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 3.000 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

TECH ist eine private Hochschuleinrichtung, die seit dem 28. Juni 2018 vom Ministerium für öffentliche Bildung anerkannt ist.

Zum 17. Juni 2020

Tere Guevara Navarro
Rektorin

Diese Qualifikation muss immer mit einem Hochschulabschluss einhergehen, der von der für die Berufsausübung zuständigen Behörde des jeweiligen Landes ausgestellt wurde. einzigartiger Code TECH: AFWOR23S techtitute.com/titel

Weiterbildender Masterstudiengang in Secure Information Management

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	ECTS	Kategorie
1°	Datenanalytik in der Unternehmensorganisation	150	OB
1°	Management und Bearbeitung von Daten und Informationen für die Datenwissenschaft	150	OB
1°	IoT-Geräte und Plattformen als Grundlage für die Datenwissenschaft	150	OB
1°	Grafische Darstellung für die Datenanalyse	150	OB
1°	Tools der Datenwissenschaft	150	OB
1°	*Data Mining.* Auswahl, Vorverarbeitung und Transformation	150	OB
1°	Vorhersagbarkeit und Analyse von stochastischen Phänomenen		
1°	Design und Entwicklung von intelligenten Systemen	150	OB
1°	Datenintensive Architekturen und Systeme	150	OB
1°	Praktische Anwendung der Datenwissenschaft in Geschäftsbereichen	150	OB
2°	Cyberintelligenz und Cybersicherheit	150	OB
2°	Host-Sicherheit	150	OB
2°	Netzwerksicherheit (Perimeter)	150	OB
2°	Smartphone-Sicherheit	150	OB
2°	IoT-Sicherheit	150	OB
2°	Ethisches *Hacking*	150	OB
2°	*Reverse Engineering*	150	OB
2°	Sichere Entwicklung	150	OB
2°	Forensische Analyse	150	OB
2°	Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit	150	OB

Tere Guevara Navarro
Rektorin

tech technologische universität

*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech technologische universität

Weiterbildender Masterstudiengang
Secure Information Management

- Modalität: **online**
- Dauer: **2 Jahre**
- Qualifizierung: **TECH Technologische Universität**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Weiterbildender Masterstudiengang

Secure Information Management

tech technologische universität