Weiterbildender Masterstudiengang

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

tech technologische universität

tech technologische universität

Weiterbildender Masterstudiengang

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

- 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-senior-cybersecurity-management-ciso-chief-information-security-officer

Index

01

Präsentation des Programms

Heutzutage ist die Cybersicherheit zu einem Grundpfeiler für den Schutz von Einzelpersonen und Unternehmen vor der wachsenden Zahl digitaler Bedrohungen geworden. Diese Disziplin konzentriert sich nicht nur auf den Schutz der technischen Systeme und kritischen Informationen von Organisationen, sondern auch auf die Planung, Umsetzung und Überwachung von Sicherheitsstrategien. Das Hauptziel besteht also darin, Risiken zu mindern und wirksam auf Cyberangriffe und -vorfälle zu reagieren. Zu den Hauptaufgaben eines Direktors für Cybersicherheit gehören die Entwicklung von Sicherheitsstrategien, das Management von technologischen Risiken und die Leitung von spezialisierten Teams. Angesichts der Herausforderungen, die sich aus dem technologischen Fortschritt und der Digitalisierung ergeben, wurde dieses Programm speziell für die Bewältigung dieser Probleme konzipiert. TECH konzentriert sich nicht nur auf die Gewährleistung eines effizienten Informationsschutzes, sondern auch auf die Erkennung und das Management neuer Schwachstellen. Damit wird der CISO zum wichtigsten Element für die Widerstandsfähigkeit jeder Organisation.

Spezialisieren Sie sich mit TECH und werden Sie führend in einem der wichtigsten Bereiche der IT“

Das Senior Cybersecurity Management ist von grundlegender Bedeutung, um die Stabilität und Kontinuität von Organisationen in einer digitalisierten und stark vernetzten Welt zu gewährleisten. Durch die Umsetzung robuster Sicherheitsstrategien und den Einsatz fortschrittlicher Technologien konnten Risiken gemindert und katastrophale Angriffe verhindert werden. In kritischen Sektoren wie dem Bankwesen, dem Gesundheitswesen und der öffentlichen Infrastruktur wurde die Sicherheit durch Governance und Compliance gestärkt, die von auf diesen Bereich spezialisierten Führungskräften vorangetrieben wurden.

Diese Disziplin hat es Unternehmen ermöglicht, sicherere digitale Arbeitsumgebungen zu schaffen und das Vertrauen von Kunden, Partnern und Nutzern zu stärken. Die erfolgreichen Ergebnisse haben zu erheblichen Einsparungen in Höhe von Millionen von Dollar an potenziellen finanziellen Verlusten geführt und gleichzeitig eine Unternehmenskultur gefördert, in der Sicherheit eine gemeinsame Priorität ist. Darüber hinaus hat es sich als wesentlich für den Schutz der Innovation, des Rufs und der Nachhaltigkeit von Unternehmen in einer sich ständig weiterentwickelnden Landschaft erwiesen.

Der weiterbildende Masterstudiengang von TECH zielt darauf ab, Fachleute auf die Leitung wirksamer Sicherheitsstrategien zu spezialisieren. Während des gesamten Programms lernen die Teilnehmer in ihrem eigenen Tempo und konzentrieren sich auf die Entwicklung von Managementfähigkeiten und strategischem Geschäftssinn. Darüber hinaus haben sie Zugang zu einer hochmodernen Spezialisierung, die sie auf eine Karriere vorbereitet, die auf dem globalen Markt sehr gefragt ist. Dank des 100%igen Online-Formats können die Teilnehmer ihr Studium mit ihren beruflichen Verpflichtungen vereinbaren, so dass sie sich weiterentwickeln können, ohne ihre berufliche Tätigkeit zu beeinträchtigen.

Dieser **Weiterbildender Masterstudiengang in Senior Cybersecurity Management (CISO, Chief Information Security Officer)** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten in Informatik präsentiert 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
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden im Senior Cybersecurity Management (CISO, Chief Information Security Officer)
- 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

Dieser weiterbildende Masterstudiengang bringt Sie an die Spitze der Branche und eröffnet Ihnen unendliche Karrieremöglichkeiten“

Entwickeln Sie die Fähigkeiten, die Sie brauchen, um die Herausforderungen der Zukunft zu meistern, ohne Ihre derzeitigen Aktivitäten zu vernachlässigen“

Werden Sie mit der Relearning-Methode, die sich an Ihr Lerntempo anpasst, zum Hüter der technologischen Infrastrukturen.

Werden Sie Teil der größten digitalen Universität der Welt und spezialisieren Sie sich von jedem Ort der Welt aus.

Zu den Dozenten gehören Fachleute aus dem Bereich des Journalismus, 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

Der Weiterbildende Masterstudiengang in Senior Cybersecurity Management (CISO) zielt auf die Spezialisierung strategischer Führungskräfte ab, die in der Lage sind, die Informationssicherheit in globalen Organisationen zu verwalten. Durch einen umfassenden und aktuellen Ansatz deckt das Programm Schlüsselbereiche wie Cybersicherheits-Governance und Risikomanagement ab. Dabei entwickeln die Studenten Managementfähigkeiten, um leistungsstarke Teams zu führen und Sicherheitsrichtlinien umzusetzen. Darüber hinaus lernen die Studenten durch die Kenntnis der neuesten Trends und aufkommenden Technologien, wie sie den Herausforderungen des digitalen Umfelds begegnen und die Sicherheit in die Zukunft führen können.

TECH bereitet Sie darauf vor, der Stratege zu sein, der Cyber-Bedrohungen im globalen Geschäftsumfeld vorbeugt, aufspürt und entschärft“

Modul 1. Cyberintelligenz und Cybersicherheit

1.1. Cyberintelligenz
- 1.1.1. Cyberintelligenz
  - 1.1.1.1. Die Intelligenz
    - 1.1.1.1.1. Intelligenz-Zyklus
  - 1.1.1.2. Cyberintelligenz
  - 1.1.1.3. Cyberintelligenz und Cybersicherheit
- 1.1.2. Der Informationsanalyst
  - 1.1.2.1. Die Rolle des Informationsanalysten
  - 1.1.2.2. Voreingenommenheit des Informationsanalysten bei der Bewertung von Aktivitäten

1.2. Cybersicherheit
- 1.2.1. Schichten der Sicherheit
- 1.2.2. Identifizierung von Cyber-Bedrohungen
  - 1.2.2.1. Externe Bedrohungen
  - 1.2.2.2. Interne Bedrohungen
- 1.2.3. Nachteilige Maßnahmen
  - 1.2.3.1. *Social Engineering*
  - 1.2.3.2. Häufig verwendete Methoden

1.3. Intelligente Tools und Techniken
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Linux-Distributionen und -Tools
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Methoden der Bewertung
- 1.4.1. Informationsanalyse
- 1.4.2. Techniken zur Organisation der erworbenen Informationen
- 1.4.3. Verlässlichkeit und Glaubwürdigkeit von Informationsquellen
- 1.4.4. Methodologien der Analyse
- 1.4.5. Präsentation der Informationsanalyse

1.5. Audits und Dokumentation
- 1.5.1. Das IT-Sicherheitsaudit
- 1.5.2. Dokumentation und Berechtigungen für Audits
- 1.5.3. Arten von Audits
- 1.5.4. Lieferbare
  - 1.5.4.1. Technischer Bericht
  - 1.5.4.2. Bericht für die Geschäftsführung

1.6. Anonymität im Netz
- 1.6.1. Nutzung der Anonymität
- 1.6.2. Anonymisierungstechniken (Proxy, VPN)
- 1.6.3. TOR, Freenet und IP2-Netzwerke

1.7. Bedrohungen und Arten von Sicherheit
- 1.7.1. Arten von Bedrohungen
- 1.7.2. Physische Sicherheit
- 1.7.3. Netzwerksicherheit
- 1.7.4. Logische Sicherheit
- 1.7.5. Sicherheit von Webanwendungen
- 1.7.6. Sicherheit für mobile Geräte

1.8. Regulierung und *Compliance*
- 1.8.1. Datenschutz-Grundverordnung
- 1.8.2. Die nationale Cybersicherheitsstrategie 2019
- 1.8.3. ISO 27000-Familie
- 1.8.4. NIST Cybersecurity Framework
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. *Cloud*-Vorschriften
- 1.8.8. SOX
- 1.8.9. ICP

1.9. Risikoanalyse und Metriken
- 1.9.1. Umfang der Risiken
- 1.9.2. Vermögenswerte
- 1.9.3. Bedrohungen
- 1.9.4. Schwachstellen
- 1.9.5. Risikobewertung
- 1.9.6. Risikobehandlung

1.10. Einschlägige Stellen für Cybersicherheit
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR - PROSUR

Modul 2. Host-Sicherheit

2.1. Sicherheitskopien
- 2.1.1. Strategien zur Datensicherung
- 2.1.2. Tools für Windows
- 2.1.3. Tools für Linux
- 2.1.4. Tools für MacOS

2.2. Benutzer-Antivirus
- 2.2.1. Arten von Antivirenprogrammen
- 2.2.2. Antivirus für Windows
- 2.2.3. Antivirus für Linux
- 2.2.4. Antivirus für MacOS
- 2.2.5. Antivirus für Smartphones

2.3. Eindringlingsdetektoren - HIDS
- 2.3.1. Methoden zur Erkennung von Eindringlingen
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Lokale Firewall
- 2.4.1. Firewalls für Windows
- 2.4.2. Firewalls für Linux
- 2.4.3. Firewalls für MacOS

2.5. Passwortmanager
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. *Phishing*-Detektoren
- 2.6.1. Manuelle *Phishing*-Erkennung
- 2.6.2. *Anti-Phishing*-Tools

2.7. Spyware
- 2.7.1. Vermeidungsmechanismen
- 2.7.2. *Anti-Spyware*-Tools

2.8. *Tracker*
- 2.8.1. Maßnahmen zum Schutz des Systems
- 2.8.2. *Anti-Tracker*-Tools

2.9. EDR - *End Point Detection and Response*
- 2.9.1. Verhalten des EDR-Systems
- 2.9.2. Unterschiede zwischen EDR und Anti-Virus
- 2.9.3. Die Zukunft der EDR-Systeme

2.10. Kontrolle über die Software-Installation
- 2.10.1. Repositorien und Software-Speicher
- 2.10.2. Listen mit erlaubter oder verbotener Software
- 2.10.3. Update-Kriterien
- 2.10.4. Berechtigungen für die Software-Installation

Modul 3. Netzwerksicherheit (Perimeter)

3.1. Systeme zur Erkennung und Abwehr von Bedrohungen
- 3.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 3.1.2. Aktuelle Verteidigungssysteme: *Defense in Depth* und SOC
- 3.1.3. Aktuelle Netzwerkarchitekturen
- 3.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
  - 3.1.4.1. Netzwerkbasierte Systeme
  - 3.1.4.2. Host-basierte Systeme
  - 3.1.4.3. Zentralisierte Systeme
- 3.1.5. Kommunikation und Erkennung von Instanzen/Hosts, Containern und Serverless

3.2. *Firewall*
- 3.2.1. Arten von *Firewalls*
- 3.2.2. Angriffe und Schadensbegrenzung
- 3.2.3. Gängige *Firewalls* in Kernel Linux
  - 3.2.3.1. UFW
  - 3.2.3.2. *Nftables und iptables*
  - 3.2.3.3. *Firewalld*
- 3.2.4. Erkennungssysteme auf der Grundlage von Systemlogs
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts und DenyHosts
  - 3.2.4.3. Fai2ban

3.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
- 3.3.1. Angriffe auf IDS/IPS
- 3.3.2. IDS/IPS-Systeme
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

3.4. *Firewalls* der nächsten Generation (NGFW)
- 3.4.1. Unterschiede zwischen NGFW und traditionellen *Firewalls*
- 3.4.2. Kernkapazitäten
- 3.4.3. Business-Lösungen
- 3.4.4. Firewalls für *Cloud*-Dienste
  - 3.4.4.1. *Cloud*-VPC-Architektur
  - 3.4.4.2. Cloud ACLs
  - 3.4.4.3. Security Group

3.5. *Proxy*
- 3.5.1. Arten von *Proxys*
- 3.5.2. *Proxy*-Nutzung. Vor- und Nachteile

3.6. Antivirus-Engines
- 3.6.1. Allgemeiner Kontext von *Malware* und IOCs
- 3.6.2. Probleme mit Anti-Viren-Programmen

3.7. Mailschutzsysteme
- 3.7.1. Antispam
  - 3.7.1.1. Schwarze und weiße Listen
  - 3.7.1.2. Bayessche Filter
- 3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Komponenten und Architektur
- 3.8.2. Korrelationsregeln und Anwendungsfälle
- 3.8.3. Aktuelle Herausforderungen von SIEM-Systemen

3.9. SOAR
- 3.9.1. SOAR und SIEM: Feinde oder Verbündete?
- 3.9.2. Die Zukunft der SOAR-Systeme

3.10. Andere netzwerkbasierte Systeme
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots und HoneyNets
- 3.10.4. CASB

Modul 4. Smartphone-Sicherheit

4.1. Die Welt der mobilen Geräte
- 4.1.1. Arten von mobilen Plattformen
- 4.1.2. IOS-Geräte
- 4.1.3. Android-Geräte

4.2. Verwaltung der mobilen Sicherheit
- 4.2.1. OWASP-Projekt für mobile Sicherheit
  - 4.2.1.1. Top 10 Schwachstellen
- 4.2.2. Kommunikation, Netzwerke und Verbindungsarten

4.3. Das mobile Gerät in der Unternehmensumgebung
- 4.3.1. Risiken
- 4.3.2. Sicherheitsrichtlinien
- 4.3.3. Geräteüberwachung
- 4.3.4. Verwaltung mobiler Geräte (MDM)

4.4. Datenschutz und Datensicherheit
- 4.4.1. Informationsstände
- 4.4.2. Datenschutz und Vertraulichkeit
  - 4.4.2.1. Zugriffsrechte
  - 4.4.2.2. Verschlüsselung
- 4.4.3. Sichere Speicherung von Daten
  - 4.4.3.1. Sichere Speicherung auf iOS
  - 4.4.3.2. Sichere Speicherung auf Android
- 4.4.4. Bewährte Praktiken bei der Applikationsentwicklung

4.5. Schwachstellen und Angriffsvektoren
- 4.5.1. Schwachstellen
- 4.5.2. Angriffsvektoren
  - 4.5.2.1. Malware
  - 4.5.2.2. Exfiltration von Daten
  - 4.5.2.3. Datenmanipulation

4.6. Wichtigste Bedrohungen
- 4.6.1. Ungezwungener Benutzer
- 4.6.2. *Malware*
  - 4.6.2.1. Arten von *Malware*
- 4.6.3. *Social Engineering*
- 4.6.4. Datenleck
- 4.6.5. Datendiebstahl
- 4.6.6. Ungesicherte WLAN-Netzwerke
- 4.6.7. Veraltete Software
- 4.6.8. Bösartige Anwendungen
- 4.6.9. Unsichere Passwörter
- 4.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen
- 4.6.11. Physischer Zugang
- 4.6.12. Verlust oder Diebstahl des Geräts
- 4.6.13. Impersonation (Integrität)
- 4.6.14. Schwache oder defekte Kryptographie
- 4.6.15. *Denial of Service* (DoS)

4.7. Große Angriffe
- 4.7.1. *Phishing*-Angriffe
- 4.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
- 4.7.3. *Smishing*-Angriffe
- 4.7.4. *Criptojacking*-Angriffe
- 4.7.5. *Man in The Middle*

4.8. Hacking
- 4.8.1. *Rooting* und *Jailbreaking*
- 4.8.2. Anatomie eines mobilen Angriffs
  - 4.8.2.1. Ausbreitung der Bedrohung
  - 4.8.2.2. Installation von *Malware* auf dem Gerät
  - 4.8.2.3. Persistenz
  - 4.8.2.4. Ausführen der *Payload* und Extrahieren der Informationen
- 4.8.3. *Hacking* auf iOS-Geräten: Mechanismen und Tools
- 4.8.4. *Hacking* auf Android-Geräten: Mechanismen und Tools

4.9. Penetrationstests
- 4.9.1. iOS *Pentesting*
- 4.9.2. Android *PenTesting*
- 4.9.3. Werkzeuge

4.10. Schutz und Sicherheit
- 4.10.1. Sicherheitseinstellungen
  - 4.10.1.1. Auf iOS-Geräten
  - 4.10.1.2. Auf Android-Geräten
- 4.10.2. Sicherheitsmaßnahmen
- 4.10.3. Schutz-Tools

Modul 5. IoT-Sicherheit

5.1. Geräte
- 5.1.1. Arten von Geräten
- 5.1.2. Standardisierte Architekturen
  - 5.1.2.1. ONEM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Anwendungsprotokolle
- 5.1.4. Konnektivitätstechnologien

5.2. IoT-Geräte. Anwendungsbereiche
- 5.2.1. *SmartHome*
- 5.2.2. *SmartCity*
- 5.2.3. Transport
- 5.2.4. *Wearables*
- 5.2.5. Gesundheitssektor
- 5.2.6. IIoT

5.3. Kommunikationsprotokolle
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Hausautomatisierung
- 5.4.2. Netzwerke
- 5.4.3. Haushaltsgeräte
- 5.4.4. Überwachung und Sicherheit

5.5. *SmartCity*
- 5.5.1. Beleuchtung
- 5.5.2. Meteorologie
- 5.5.3. Sicherheit

5.6. Transport
- 5.6.1. Standort
- 5.6.2. Zahlungen leisten und Dienstleistungen in Anspruch nehmen
- 5.6.3. Konnektivität

5.7. *Wearables*
- 5.7.1. Intelligente Kleidung
- 5.7.2. Intelligenter Schmuck
- 5.7.3. Intelligente Uhren

5.8. Gesundheitssektor
- 5.8.1. Training/Herzfrequenzüberwachung
- 5.8.2. Überwachung von Patienten und älteren Menschen
- 5.8.3. Implantierbare Geräte
- 5.8.4. Chirurgische Roboter

5.9. Konnektivität
- 5.9.1. WLAN/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Eingebettete Konnektivität

5.10. Sicherung
- 5.10.1. Dedizierte Netzwerke
- 5.10.2. Passwortmanager
- 5.10.3. Verwendung von verschlüsselten Protokollen
- 5.10.4. Tipps für die Verwendung

Modul 6. Ethisches *Hacking*

6.1. Arbeitsumgebung
- 6.1.1. Linux-Distributionen
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Virtualisierungssysteme
- 6.1.3. *Sandbox*
- 6.1.4. Einsatz von Labors

6.2. Methoden
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. *Open Source Intelligence* (OSINT)
- 6.3.2. Suche nach Datenschutzverletzungen und Schwachstellen
- 6.3.3. Verwendung von passiven Tools

6.4. Netzwerk-Scans
- 6.4.1. Tools zum Scannen
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Andere Scan-Tools
- 6.4.2. Scanning-Techniken
- 6.4.3. Techniken zur Umgehung von *Firewalls* und IDS
- 6.4.4. *Banner Grabbing*
- 6.4.5. Netzwerk-Diagramme

6.5. Aufzählung
- 6.5.1. SMTP-Aufzählung
- 6.5.2. DNS-Aufzählung
- 6.5.3. NetBIOS- und Samba-Aufzählung
- 6.5.4. LDAP-Aufzählung
- 6.5.5. SNMP-Aufzählung
- 6.5.6. Andere Aufzählungstechniken

6.6. Scannen auf Schwachstellen
- 6.6.1. Lösungen zum Scannen auf Schwachstellen
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Systeme zur Bewertung von Schwachstellen
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Angriffe auf drahtlose Netzwerke
- 6.7.1. Methodik zum Hacken drahtloser Netzwerke
  - 6.7.1.1. WLAN *Discovery*
  - 6.7.1.2. Verkehrsanalyse
  - 6.7.1.3. *Aircrack*-Angriffe
    - 6.7.1.3.1. WEP-Angriffe
    - 6.7.1.3.2. WPA/WPA2-Angriffe
  - 6.7.1.4. *Evil-Twin*-Angriffe
  - 6.7.1.5. WPS-Angriffe
  - 6.7.1.6. *Jamming*
- 6.7.2. Tools für drahtlose Sicherheit

6.8. *Hacking* von Webservern
- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQLinjection*

6.9. Ausnutzung von Schwachstellen
- 6.9.1. Verwendung von bekannten *Exploits*
- 6.9.2. Verwendung von *Metasploit*
- 6.9.3. Verwendung von *Malware*
  - 6.9.3.1. Definition und Umfang
  - 6.9.3.2. Generierung von *Malware*
  - 6.9.3.3. Umgehung von Anti-Virus-Lösungen

6.10. Persistenz
- 6.10.1. Installation von *Rootkits*
- 6.10.2. Verwendung von Ncat
- 6.10.3. Verwendung von geplanten Aufgaben für Backdoors
- 6.10.4. Benutzer erstellen
- 6.10.5. HIDS aufspüren

Modul 7. *Reverse Engineering*

7.1. *Compiler*
- 7.1.1. Arten von Code
- 7.1.2. *Compiler*-Phasen
- 7.1.3. Symboltabelle
- 7.1.4. Fehler-Handler
- 7.1.5. GCC Compiler

7.2. Arten der *Compiler*-Analyse
- 7.2.1. Lexikalische Analyse
  - 7.2.1.1. Terminologie
  - 7.2.1.2. Lexikalische Komponenten
  - 7.2.1.3. LEX. Lexikalischer Analysator
- 7.2.2. Syntaktische Analyse
  - 7.2.2.1. Kontextfreie Grammatiken
  - 7.2.2.2. Arten des *Parsing*
    - 7.2.2.2.1. Top-down-*Parsing*
    - 7.2.2.2.2. Bottom-up-*Parsing*
  - 7.2.2.3. Syntaktische Bäume und Ableitungen
  - 7.2.2.4. Arten von *Parsern*
    - 7.2.2.4.1. LR-*Parser* (*Left to Right*)
    - 7.2.2.4.2. LALR-*Parser*
- 7.2.3. Semantische Analyse
  - 7.2.3.1. Attribut-Grammatiken
  - 7.2.3.2. S-Attribute
  - 7.2.3.3. L-Attribute

7.3. Montage-Datenstrukturen
- 7.3.1. Variablen
- 7.3.2. Arrays
- 7.3.3. Zeiger
- 7.3.4. Strukturen
- 7.3.5. Objekte

7.4. *Assembly-Code*-Strukturen
- 7.4.1. Auswahl-Strukturen
  - 7.4.1.1. *If, else if, Else*
  - 7.4.1.2. *Switch*
- 7.4.2. Iterations-Strukturen
  - 7.4.2.1. *For*
  - 7.4.2.2. *While*
  - 7.4.2.3. Verwendung des *Break*
- 7.4.3. Funktionen

7.5. x86-Hardware-Architektur
- 7.5.1. x86-Prozessorarchitektur
- 7.5.2. x86-Datenstrukturen
- 7.5.3. x86-Codestrukturen
- 7.5.3. x86-Codestrukturen

7.6. ARM-Hardwarearchitektur
- 7.6.1. ARM-Prozessorarchitektur
- 7.6.2. ARM-Datenstrukturen
- 7.6.3. ARM-Codestrukturen

7.7. Statische Codeanalyse
- 7.7.1. *Disassembler*
- 7.7.2. IDA
- 7.7.3. Code-Rekonstrukteure

7.8. Dynamische Codeanalyse
- 7.8.1. Verhaltensanalyse
  - 7.8.1.1. Kommunikation
  - 7.8.1.2. Überwachung
- 7.8.2. Linux-Code-Debugger
- 7.8.3. Windows-Code-Debugger

7.9. Sandbox
- 7.9.1. *Sandbox*-Architektur
- 7.9.2. *Sandbox*-Umgehung
- 7.9.3. Erkennungstechniken
- 7.9.4. Ausweichtechniken
- 7.9.5. Gegenmaßnahmen
- 7.9.6. Sandbox in Linux
- 7.9.7. Sandbox in Windows
- 7.9.8. Sandbox in MacOS
- 7.9.9. Sandbox in Android

7.10. *Malware*-Scans
- 7.10.1. Methoden zur Analyse des *Malware*
- 7.10.2. Techniken zur Verschleierung von *Malware*
  - 7.10.2.1. Ausführbare Verschleierung
  - 7.10.2.2. Einschränkung der Ausführungsumgebungen
- 7.10.3. Tools zur Analyse des *Malware*

Modul 8. Sichere Entwicklung

8.1. Sichere Entwicklung
- 8.1.1. Qualität, Funktionalität und Sicherheit
- 8.1.2. Vertraulichkeit, Integrität und Verfügbarkeit
- 8.1.3. Lebenszyklus der Softwareentwicklung

8.2. Phase der Anforderungen
- 8.2.1. Kontrolle der Authentifizierung
- 8.2.2. Kontrolle von Rollen und Privilegien
- 8.2.3. Risikoorientierte Anforderungen
- 8.2.4. Genehmigung von Privilegien

8.3. Analyse- und Entwurfsphasen
- 8.3.1. Komponentenzugriff und Systemverwaltung
- 8.3.2. Prüfpfade
- 8.3.3. Sitzungsmanagement
- 8.3.4. Historische Daten
- 8.3.5. Angemessene Fehlerbehandlung
- 8.3.6. Trennung der Funktionen

8.4. Phase der Implementierung und Kodierung
- 8.4.1. Absicherung der Entwicklungsumgebung
- 8.4.2. Ausarbeitung der technischen Dokumentation
- 8.4.3. Sichere Kodierung
- 8.4.4. Sicherheit der Kommunikation

8.5. Gute sichere Kodierungspraktiken
- 8.5.1. Validierung von Eingabedaten
- 8.5.2. Verschlüsselung der Ausgabedaten
- 8.5.3. Programmierstil
- 8.5.4. Handhabung des Änderungsprotokolls
- 8.5.5. Kryptographische Praktiken
- 8.5.6. Fehler- und Protokollverwaltung
- 8.5.7. Dateiverwaltung
- 8.5.8. Speicherverwaltung
- 8.5.9. Standardisierung und Wiederverwendung von Sicherheitsfunktionen

8.6. Vorbereitung und *Hardening* von Servern
- 8.6.1. Verwaltung von Benutzern, Gruppen und Rollen auf dem Server
- 8.6.2. Software-Installation
- 8.6.3. *Hardening* des Servers
- 8.6.4. Robuste Konfiguration der Anwendungsumgebung

8.7. DB-Vorbereitung und *Hardening*
- 8.7.1. Optimierung der DB-Engine
- 8.7.2. Erstellung eines eigenen Benutzers für die Anwendung
- 8.7.3. Zuweisung der erforderlichen Berechtigungen an den Benutzer
- 8.7.4. *Hardening* der DB

8.8. Testphase
- 8.8.1. Qualitätskontrolle bei Sicherheitskontrollen
- 8.8.2. Stufenweise Code-Inspektion
- 8.8.3. Überprüfung der Konfigurationsverwaltung
- 8.8.4. Black-Box-Tests

8.9. Vorbereitungen für den Übergang zur Produktion
- 8.9.1. Änderungskontrolle durchführen
- 8.9.2. Durchführen der Produktionsumstellung
- 8.9.3. *Rollback*-Prozedur durchführen
- 8.9.4. Tests in der Vorproduktionsphase

8.10. Erhaltungsphase
- 8.10.1. Risikobasierte Versicherung
- 8.10.2. White-Box-Tests zur Wartung der Sicherheit
- 8.10.3. Black-Box-Tests zur Wartung der Sicherheit

Modul 9. Praktische Implementierung von Sicherheitsrichtlinien für Software und Hardware

9.1. Praktische Implementierung von Sicherheitsrichtlinien für Software und Hardware
- 9.1.1. Implementierung von Identifizierung und Autorisierung
- 9.1.2. Implementierung von Identifizierungstechniken
- 9.1.3. Technische Maßnahmen zur Autorisierung

9.2. Identifizierungs- und Autorisierungstechniken
- 9.2.1. Kennung und OTP
- 9.2.2. USB-Token oder PKI-Smartcard
- 9.2.3. Der Schlüssel „Vertrauliche Verteidigung"
- 9.2.4. Aktive RFID

9.3. Sicherheitspolitiken für den Zugang zu Software und Systemen
- 9.3.1. Implementierung von Politiken zur Zugriffskontrolle
- 9.3.2. Umsetzung von Politiken für den Zugang zur Kommunikation
- 9.3.3. Arten von Sicherheitstools für die Zugriffskontrolle

9.4. Verwaltung des Benutzerzugriffs
- 9.4.1. Verwaltung von Zugriffsrechten
- 9.4.2. Trennung von Rollen und Zugriffsfunktionen
- 9.4.3. Implementierung von Zugriffsrechten in Systemen

9.5. Kontrolle des Zugriffs auf Systeme und Anwendungen
- 9.5.1. Mindestzugriffsregel
- 9.5.2. Sichere Anmeldetechnologien
- 9.5.3. Passwort-Sicherheitsrichtlinien

9.6. Technologien für Identifikationssysteme
- 9.6.1. Aktives Verzeichnis
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. CIS-Kontrollen für Bastionierungssysteme
- 9.7.1. Allgemeine CIS-Kontrollen
- 9.7.2. Grundlegende CIS-Kontrollen
- 9.7.3. Organisatorische CIS-Kontrollen

9.8. Operative Sicherheit
- 9.8.1. Schutz vor bösartigem Code
- 9.8.2. Sicherheitskopien
- 9.8.3. Aktivitätsprotokollierung und Überwachung

9.9. Management von technischen Schwachstellen
- 9.9.1. Technische Schwachstellen
- 9.9.2. Management von technischen Schwachstellen
- 9.9.3. Einschränkungen bei der Software-Installation

9.10. Umsetzung der Sicherheitspraktiken
- 9.10.1. Logische Schwachstellen
- 9.10.2. Implementierung von Verteidigungsrichtlinien

Modul 10. Forensische Analyse

10.1. Datenerfassung und Replikation
- 10.1.1. Volatile Datenerfassung
  - 10.1.1.1. System-Informationen
  - 10.1.1.2. Netzwerk-Informationen
  - 10.1.1.3. Reihenfolge der Volatilität
- 10.1.2. Statische Datenerfassung
  - 10.1.2.1. Erstellung eines doppelten Bildes
  - 10.1.2.2. Erstellung eines Dokuments für die Überwachungskette
- 10.1.3. Methoden zur Validierung der erfassten Daten
  - 10.1.3.1. Methoden für Linux
  - 10.1.3.2. Methoden für Windows

10.2. Bewertung und Beseitigung von Anti-Forensik-Techniken
- 10.2.1. Ziele der forensischen Techniken
- 10.2.2. Löschung von Daten
  - 10.2.2.1. Löschung von Daten und Dateien
  - 10.2.2.2. Dateiwiederherstellung
  - 10.2.2.3. Wiederherstellung von gelöschten Partitionen
- 10.2.3. Passwortschutz
- 10.2.4. Steganographie
- 10.2.5. Sicheres Löschen von Geräten
- 10.2.6. Verschlüsselung

10.3. Betriebssystem-Forensik
- 10.3.1. Windows-Forensik
- 10.3.2. Linux-Forensik
- 10.3.3. Mac-Forensik

10.4. Netzwerk-Forensik
- 10.4.1. Log-Analyse
- 10.4.2. Korrelation der Daten
- 10.4.3. Netzwerk-Untersuchung
- 10.4.4. Schritte der forensischen Netzwerkanalyse

10.5. Web-Forensik
- 10.5.1. Untersuchung von Webangriffen
- 10.5.2. Angriffserkennung
- 10.5.3. Standort der IP-Adresse

10.6. Datenbank-Forensik
- 10.6.1. MSSQL-Forensik
- 10.6.2. MySQL-Forensik
- 10.6.3. PostgreSQL-Forensik
- 10.6.4. MongoDB-Forensik

10.7. Cloud-Forensik
- 10.7.1. Arten von *Cloud*-Verbrechen
  - 10.7.1.1. *Cloud* als Thema
  - 10.7.1.2. *Cloud* als Objekt
  - 10.7.1.3. *Cloud* als Werkzeug
- 10.7.2. Herausforderungen der *Cloud*-Forensik
- 10.7.3. Untersuchung von *Cloud*-Speicherdiensten
- 10.7.4. Forensische Analyse-Tools für die *Cloud*

10.8. Untersuchung von E-Mail-Verbrechen
- 10.8.1. Mail-Systeme
  - 10.8.1.1. *Mail Clients*
  - 10.8.1.2. Mail-Server
  - 10.8.1.3. SMTP-Server
  - 10.8.1.4. POP3-Server
  - 10.8.1.5. IMAP4-Server
- 10.8.2. Mail-Verbrechen
- 10.8.3. Mail-Nachricht
  - 10.8.3.1. Standard-Kopfzeilen
  - 10.8.3.2. Erweiterte Kopfzeilen
- 10.8.4. Schritte bei der Untersuchung dieser Verbrechen
- 10.8.5. Tools für die E-Mail-Forensik

10.9. Mobile forensische Analyse
- 10.9.1. Zellulare Netzwerke
  - 10.9.1.1. Arten von Netzwerken
  - 10.9.1.2. CDR-Inhalt
- 10.9.2. *Subscriber Identity Module* (SIM)
- 10.9.3. Logische Akquisition
- 10.9.4. Physische Akquisition
- 10.9.5. Dateisystem-Erfassung

10.10. Forensische Berichte schreiben und einreichen
- 10.10.1. Wichtige Aspekte eines forensischen Berichts
- 10.10.2. Klassifizierung und Arten von Berichten
- 10.10.3. Leitfaden zum Schreiben eines Berichts
- 10.10.4. Präsentation des Berichts
  - 10.10.4.1. Vorbereitung auf die Zeugenaussage
  - 10.10.4.2. Hinterlegung
  - 10.10.4.3. Der Umgang mit den Medien

Modul 11. Sicherheit in Design und Entwicklung von Systemen

11.1. Informationssysteme
- 11.1.1. Domains eines Informationssystems
- 11.1.2. Komponenten eines Informationssystems
- 11.1.3. Aktivitäten eines Informationssystems
- 11.1.4. Lebenszyklus eines Informationssystems
- 11.1.5. Ressourcen eines Informationssystems

11.2. Informationssysteme. Typologie
- 11.2.1. Typen von Informationssystemen
  - 11.2.1.1. Unternehmerisch
  - 11.2.1.2. Strategisch
  - 11.2.1.3. Je nach Anwendungsbereich
  - 11.2.1.4. Spezifisch
- 11.2.2. Informationssysteme. Beispiele aus der Praxis
- 11.2.3. Entwicklung von Informationssystemen: Phasen
- 11.2.4. Methoden der Informationssysteme

11.3. Sicherheit von Informationssystemen. Rechtliche Implikationen
- 11.3.1. Zugang zu Daten
- 11.3.2. Sicherheitsbedrohungen: Schwachstellen
- 11.3.3. Rechtliche Implikationen: Straftaten
- 11.3.4. Verfahren zur Wartung von Informationssystemen

11.4. Sicherheit von Informationssystemen. Sicherheitsprotokolle
- 11.4.1. Sicherheit von Informationssystemen
  - 11.4.1.1. Integrität
  - 11.4.1.2. Vertraulichkeit
  - 11.4.1.3. Verfügbarkeit
  - 11.4.1.4. Authentifizierung
- 11.4.2. Sicherheitsdienste
- 11.4.3. Protokolle zur Informationssicherheit. Typologie
- 11.4.4. Empfindlichkeit von Informationssystemen

11.5. Sicherheit von Informationssystemen. Maßnahmen und Systeme zur Zugangskontrolle
- 11.5.1. Sicherheitsmaßnahmen
- 11.5.2. Art der Sicherheitsmaßnahmen
  - 11.5.2.1. Prävention
  - 11.5.2.2. Erkennung
  - 11.5.2.3. Korrektheit
- 11.5.3. Kontrollsysteme für den Zugang. Typologie
- 11.5.4. Kryptographie

11.6. Netzwerk- und Internetsicherheit
- 11.6.1. *Firewalls*
- 11.6.2. Digitale Identifizierung
- 11.6.3. Viren und Würmer
- 11.6.4. *Hacking*
- 11.6.5. Beispiele und reale Fälle

11.7. Computerkriminalität
- 11.7.1. Computerkriminalität
- 11.7.2. Computerkriminalität. Typologie
- 11.7.3. Computerkriminalität. Angriff. Typologien
- 11.7.4. Der Fall der virtuellen Realität
- 11.7.5. Profile von Tätern und Opfern. Typisierung von Verbrechen
- 11.7.6. Computerkriminalität. Beispiele und reale Fälle

11.8. Sicherheitsplan für ein Informationssystem
- 11.8.1. Sicherheitsplan. Ziele
- 11.8.2. Sicherheitsplan. Planung
- 11.8.3. Risikoplan. Analyse
- 11.8.4. Sicherheitspolitik. Implementierung in der Organisation
- 11.8.5. Sicherheitsplan. Implementierung in der Organisation
- 11.8.6. Sicherheitsverfahren. Arten
- 11.8.7. Sicherheitsplan. Beispiele

11.9. Plan für unvorhergesehene Ereignisse
- 11.9.1. Plan für unvorhergesehene Ereignisse. Funktionen
- 11.9.2. Notfallplan: Elemente und Ziele
- 11.9.3. Plan für unvorhergesehene Ereignisse in der Organisation. Implementierung
- 11.9.4. Plan für unvorhergesehene Ereignisse. Beispiele

11.10. Verwaltung der Sicherheit von Informationssystemen
- 11.10.1. Gesetzliche Bestimmungen
- 11.10.2. Normen
- 11.10.3. Zertifizierungen
- 11.10.4. Technologien

Modul 12. Architekturen und Modelle für die Informationssicherheit

12.1. Architektur der Informationssicherheit
- 12.1.1. ISMS / ISDP
- 12.1.2. Strategische Ausrichtung
- 12.1.3. Risikomanagement
- 12.1.4. Leistungsmessung

12.2. Modelle der Informationssicherheit
- 12.2.1. Richtlinienbasierte Sicherheitsmodelle
- 12.2.2. Basierend auf Schutz-Tools
- 12.2.3. Teambasiert

12.3. Sicherheitsmodell. Wichtige Komponenten
- 12.3.1. Identifizierung von Risiken
- 12.3.2. Definition von Kontrollen
- 12.3.3. Kontinuierliche Bewertung des Risikoniveaus
- 12.3.4. Sensibilisierungsplan für Mitarbeiter, Lieferanten, Partner usw.

12.4. Prozess der Risikoverwaltung
- 12.4.1. Identifizierung von Vermögenswerten
- 12.4.2. Identifizierung von Bedrohungen
- 12.4.3. Risikobewertung
- 12.4.4. Priorisierung der Kontrollen
- 12.4.5. Neubeurteilung und Restrisiko

12.5. Geschäftsprozesse und Informationssicherheit
- 12.5.1. Geschäftsprozesse
- 12.5.2. Risikobewertung auf der Grundlage geschäftlicher Parameter
- 12.5.3. Analyse der Auswirkungen auf das Geschäft
- 12.5.4. Geschäftsbetrieb und Informationssicherheit

12.6. Prozess zur kontinuierlichen Verbesserung
- 12.6.1. Der Deming-Zyklus
  - 12.6.1.1. Planung
  - 12.6.1.2. Machen
  - 12.6.1.3. Prüfen
  - 12.6.1.4. Agieren

12.7. Sicherheitsarchitekturen
- 12.7.1. Auswahl und Homogenisierung von Technologien
- 12.7.2. Identitätsmanagement. Authentifizierung
- 12.7.3. Zugriffsverwaltung. Autorisierung
- 12.7.4. Sicherheit der Netzwerkinfrastruktur
- 12.7.5. Verschlüsselungstechnologien und -lösungen
- 12.7.6. Sicherheit der Endgeräte (EDR)

12.8. Der rechtliche Rahmen
- 12.8.1. Regulatorischer Rahmen
- 12.8.2. Zertifizierungen
- 12.8.3. Gesetzgebung

12.9. Der ISO 27001-Standard
- 12.9.1. Implementierung
- 12.9.2. Zertifizierung
- 12.9.3. Audits und Penetrationstests
- 12.9.4. Laufendes Risikomanagement
- 12.9.5. Klassifizierung der Informationen

12.10. Gesetzgebung zum Datenschutz. RGPD (GDPR)
- 12.10.1. Anwendungsbereich der Allgemeinen Datenschutzverordnung (GDPR)
- 12.10.2. Persönliche Daten
- 12.10.3. Rollen bei der Verarbeitung von personenbezogenen Daten
- 12.10.4. ARCO-Rechte
- 12.10.5. Der DPO. Funktionen

Modul 13. Informationssicherheits-Managementsystem (ISMS)

13.1. Informationssicherheit. Schlüsselaspekte
- 13.1.1. Informationssicherheit
  - 13.1.1.1. Vertraulichkeit
  - 13.1.1.2. Integrität
  - 13.1.1.3. Verfügbarkeit
  - 13.1.1.4. Maßnahmen zur Informationssicherheit

13.2. Managementsystem für die Informationssicherheit
- 13.2.1. Modelle für das Management der Informationssicherheit
- 13.2.2. Dokumente für die Implementierung eines ISMS
- 13.2.3. ISMS-Stufen und Kontrollen

13.3. Internationale Normen und Standards
- 13.3.1. Internationale Normen zur Informationssicherheit
- 13.3.2. Ursprung und Entwicklung des Standards
- 13.3.3. Internationale Standards für das Management der Informationssicherheit
- 13.3.4. Andere Referenzstandards

13.4. ISO/IEC 27000-Normen
- 13.4.1. Zweck und Anwendungsbereich
- 13.4.2. Aufbau der Norm
- 13.4.3. Zertifizierung
- 13.4.4. Phasen der Akkreditierung
- 13.4.5. Vorteile der ISO/IEC 27000-Normen

13.5. Entwurf und Implementierung eines allgemeinen Informationssicherheitssystems
- 13.5.1. Phasen der Implementierung eines allgemeinen Informationssicherheitssystems
- 13.5.2. *Business Continuity Plan*

13.6. Phase I: Diagnose
- 13.6.1. Vorläufige Diagnose
- 13.6.2. Identifizierung der Ebene der Schichtung
- 13.6.3. Grad der Einhaltung von Standards/Normen

13.7. Phase II: Vorbereitung
- 13.7.1. Organisatorischer Kontext
- 13.7.2. Analyse der geltenden Sicherheitsvorschriften
- 13.7.3. Umfang des gesamten Informationssicherheitssystems
- 13.7.4. Allgemeine Richtlinien für das Informationssicherheitssystem
- 13.7.5. Zielsetzungen des allgemeinen Informationssicherheitssystems

13.8. Phase III: Planung
- 13.8.1. Klassifizierung der Vermögenswerte
- 13.8.2. Risikobewertung
- 13.8.3. Identifizierung von Bedrohungen und Risiken

13.9. Phase IV: Umsetzung und Überwachung
- 13.9.1. Analyse der Ergebnisse
- 13.9.2. Zuweisung von Verantwortlichkeiten
- 13.9.3. Zeitplan für den Aktionsplan
- 13.9.4. Überwachung und Audits

13.10. Sicherheitsrichtlinien für das Incident Management
- 13.10.1. Phasen
- 13.10.2. Kategorisierung von Vorfällen
- 13.10.3. Verfahren für Zwischenfälle und Zwischenfallmanagement

Modul 14. IT-Sicherheitsmanagement

14.1. Sicherheitsmanagement
- 14.1.1. Sicherheitsmaßnahmen
- 14.1.2. Rechtliche und regulatorische Aspekte
- 14.1.3. Geschäftliche Freigabe
- 14.1.4. Risikomanagement
- 14.1.5. Identitäts- und Zugriffsmanagement

14.2. Struktur des Sicherheitsbereichs. Das Büro des CISO
- 14.2.1. Organisatorische Struktur. Position des CISO in der Struktur
- 14.2.2. Verteidigungslinien
- 14.2.3. Organigramm des Büros des CISO
- 14.2.4. Haushaltsführung

14.3. Sicherheitsmanagement
- 14.3.1. Sicherheitsausschuss
- 14.3.2. Ausschuss für Risikoüberwachung
- 14.3.3. Prüfungsausschuss
- 14.3.4. Krisenausschuss

14.4. *Security Governance*. Funktionen
- 14.4.1. Politiken und Standards
- 14.4.2. Masterplan für Sicherheit
- 14.4.3. *Dashboards*
- 14.4.4. Sensibilisierung und Schulung
- 14.4.5. Sicherheit der Lieferkette

14.5. Sicherheitsmaßnahmen
- 14.5.1. Identitäts- und Zugriffsmanagement
- 14.5.2. Konfiguration von Netzwerksicherheitsregeln. *Firewalls*
- 14.5.3. Verwaltung der IDS/IPS-Plattform
- 14.5.4. Scannen auf Schwachstellen

14.6. Cybersecurity-Rahmenwerk. NIST CSF
- 14.6.1. NIST-Methodik
  - 14.6.1.1. Identifizieren
  - 14.6.1.2. Schützen
  - 14.6.1.3. Erkennen
  - 14.6.1.4. Reagieren
  - 14.6.1.5. Zurückgewinnen

14.7. Sicherheitsoperationszentrum (SOC). Funktionen
- 14.7.1. Schutz. *Red Team*, *Pentesting*, *Threat Intelligence*
- 14.7.2. Erkennung. SIEM, *User Behavior Analytics*, *Fraud Prevention*
- 14.7.3. Antwort

14.8. Sicherheitsaudits
- 14.8.1. Penetrationstests
- 14.8.2. Übungen des *Red Team*
- 14.8.3. Quellcode-Prüfungen. Sichere Entwicklung
- 14.8.4. Komponentensicherheit (*Software Supply Chain*)
- 14.8.5. Forensische Analyse

14.9. Reaktion auf Vorfälle
- 14.9.1. Vorbereitung
- 14.9.2. Erkennung, Analyse und Berichterstattung
- 14.9.3. Eindämmung, Ausrottung und Wiederherstellung
- 14.9.4. Aktivitäten nach dem Vorfall
  - 14.9.4.1. Aufbewahrung von Beweisen
  - 14.9.4.2. Forensische Analyse
  - 14.9.4.3. Lücken-Management
- 14.9.5. Offizielle Leitfäden für das Management von Cybervorfällen

14.10. Management von Schwachstellen
- 14.10.1. Scannen auf Schwachstellen
- 14.10.2. Bewertung der Anfälligkeit
- 14.10.3. Verstärkung des Systems
- 14.10.4. *Zero-Day*-Sicherheitslücken. *Zero-Day*

Modul 15. Richtlinien für das Management von Sicherheitsvorfällen

15.1. Richtlinien und Verbesserungen für das Management von Sicherheitsvorfällen in der Informationssicherheit
- 15.1.1. Management von Zwischenfällen
- 15.1.2. Verantwortlichkeiten und Verfahren
- 15.1.3. Event-Benachrichtigung

15.2. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
- 15.2.1. Daten zur Systemleistung
- 15.2.2. Arten von Intrusion Detection Systemen
- 15.2.3. Kriterien für den Standort von IDS/IPS

15.3. Reaktion auf Sicherheitsvorfälle
- 15.3.1. Verfahren zum Sammeln von Informationen
- 15.3.2. Verfahren zur Überprüfung der Intrusion
- 15.3.3. CERT-Gremien

15.4. Benachrichtigung über einen Einbruchsversuch und Managementprozess
- 15.4.1. Verantwortlichkeiten im Benachrichtigungsprozess
- 15.4.2. Klassifizierung von Vorfällen
- 15.4.3. Lösung und Wiederherstellungsprozess

15.5. Forensische Analyse als Sicherheitspolitik
- 15.5.1. Volatile und nichtvolatile Beweise
- 15.5.2. Analyse und Sammlung von elektronischen Beweismitteln
  - 15.5.2.1. Analyse von elektronischen Beweismitteln
  - 15.5.2.2. Sammlung von elektronischen Beweismitteln

15.6. Tools für Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Tools zur Zentralisierung von Ereignissen
- 15.7.1. SIM
- 15.7.2. SEM
- 15.7.3. SIEM

15.8. Sicherheitsleitfaden CCN-STIC 817
- 15.8.1. Management von Cybervorfällen
- 15.8.2. Metriken und Indikatoren

15.9. NIST SP800-61
- 15.9.1. Fähigkeit zur Reaktion auf Computer-Sicherheitsvorfälle
- 15.9.2. Umgang mit einem Vorfall
- 15.9.3. Koordinierung und Informationsaustausch

15.10. ISO 27035-Norm
- 15.10.1. ISO 27035-Norm. Grundsätze des Vorfallsmanagements
- 15.10.2. Richtlinien für die Entwicklung eines Vorfallsmanagementplans
- 15.10.3. Richtlinien für die Reaktion auf Vorfälle

Modul 16. Risikoanalyse und IT-Sicherheitsumgebung

16.1. Analyse des Umfelds
- 16.1.1. Analyse der wirtschaftlichen Lage
  - 16.1.1.1. VUCA-Umgebungen
    - 16.1.1.1.1. Volatil
    - 16.1.1.1.2. Ungewiss
    - 16.1.1.1.3. Komplex
    - 16.1.1.1.4. Mehrdeutig
  - 16.1.1.2. BANI-Umgebungen
    - 16.1.1.2.1. Spröde
    - 16.1.1.2.2. Ängstlich
    - 16.1.1.2.3. Nicht linear
    - 16.1.1.2.4. Unverständlich

16.1.2. Analyse des allgemeinen Umfelds. PESTEL
16.1.2.1. Politisch
16.1.2.2. Wirtschaftlich
16.1.2.3. Sozial
16.1.2.4. Technologisch
16.1.2.5. Ökologisch/Umweltbezogen
16.1.2.6. Rechtlich
16.1.3. Analyse der internen Situation. SWOT
16.1.3.1. Ziele
16.1.3.2. Bedrohungen
16.1.3.3. Gelegenheiten
16.1.3.4. Stärken
16.2. Risiko und Ungewissheit
16.2.1. Risiko
16.2.2. Risikomanagement
16.2.3. Standards für das Risikomanagement
16.3. Richtlinien zum Risikomanagement ISO 31.000:2018
16.3.1. Gegenstand
16.3.2. Grundsätze
16.3.3. Referenzrahmen
16.3.4. Prozess
16.4. Methodik für die Analyse und das Management von Risiken in Informationssystemen (MAGERIT)
16.4.1. MAGERIT-Methodik
16.4.1.1. Ziele
16.4.1.2. Methode
16.4.1.3. Elemente
16.4.1.4. Techniken
16.4.1.5. Verfügbare Tools (PILAR)
16.5. Übertragung von Cyberrisiken
16.5.1. Risikotransfer
16.5.2. Cyberrisiken. Typologie
16.5.3. Versicherung gegen Cyberrisiken
16.6. Agile Methoden für das Risikomanagement
16.6.1. Agile Methoden
16.6.2. Scrum für das Risikomanagement
16.6.3. *Agile Risk Management*
16.7. Technologien für das Risikomanagement
16.7.1. Künstliche Intelligenz für das Risikomanagement
16.7.2. *Blockchain* und Kryptographie. Methoden zur Werterhaltung
16.7.3. Quantencomputing. Potenzial oder Bedrohung
16.8. IT-Risiko-*Mapping* auf der Grundlage agiler Methoden
16.8.1. Darstellung von Wahrscheinlichkeiten und Auswirkungen in agilen Umgebungen
16.8.2. Risiko als Bedrohung für den Wert
16.8.3. Neuentwicklung von agilem Projektmanagement und agilen Prozessen auf der Grundlage von KRIs
16.9. *Risk Driven* im Risikomanagement
16.9.1. *Risk Driven*
16.9.2. *Risk Driven* im Risikomanagement
16.9.3. Entwicklung eines risikoorientierten Geschäftsführungsmodells
16.10. Innovation und digitale Transformation im IT-Risikomanagement
16.10.1. Agiles Risikomanagement als Quelle für geschäftliche Innovation
16.10.2. Umwandlung von Daten in entscheidungsrelevante Informationen
16.10.3. Ganzheitliche Betrachtung des Unternehmens durch Risiko

Modul 17. Sicherheitsrichtlinien für die Analyse von Bedrohungen in Computersystemen

17.1. Bedrohungsmanagement in Sicherheitsrichtlinien
17.1.1. Das Risikomanagement
17.1.2. Das Sicherheitsrisiko
17.1.3. Methodologien im Bedrohungsmanagement
17.1.4. Implementierung von Methoden
17.2. Phasen des Managements von Bedrohungen
17.2.1. Identifizierung
17.2.2. Analyse
17.2.3. Standort
17.2.4. Schutzmaßnahmen
17.3. Auditsysteme zur Lokalisierung von Bedrohungen
17.3.1. Klassifizierung und Informationsfluss
17.3.2. Analyse der anfälligen Prozesse

17.4. Risikoklassifizierung
- 17.4.1. Arten von Risiko
- 17.4.2. Berechnung der Gefahrenwahrscheinlichkeit
- 17.4.3. Residuales Risiko

17.5. Risikobehandlung
- 17.5.1. Umsetzung von Schutzmaßnahmen
- 17.5.2. Übertragung oder Übernahme

17.6. Risikokontrolle
- 17.6.1. Kontinuierlicher Risikomanagementprozess
- 17.6.2. Implementierung von Sicherheitsmetriken
- 17.6.3. Strategisches Modell der Metriken für die Informationssicherheit

17.7. Praktische Methoden für die Analyse und Kontrolle von Bedrohungen
- 17.7.1. Katalog der Bedrohungen
- 17.7.2. Katalog der Kontrollmaßnahmen
- 17.7.3. Katalog der Sicherheitsvorkehrungen

17.8. ISO 27005-Norm
- 17.8.1. Identifizierung von Risiken
- 17.8.2. Risikoanalyse
- 17.8.3. Risikobewertung

17.9. Matrix der Risiken, Auswirkungen und Bedrohungen
- 17.9.1. Daten, Systeme und Personal
- 17.9.2. Wahrscheinlichkeit der Bedrohung
- 17.9.3. Ausmaß des Schadens

17.10. Gestaltung von Phasen und Prozessen in der Gefahrenanalyse
- 17.10.1. Identifizierung der kritischen Elemente der Organisation
- 17.10.2. Bestimmung der Bedrohungen und Auswirkungen
- 17.10.3. Analyse der Auswirkungen und Risiken
- 17.10.4. Methoden

Modul 18. Praktische Implementierung von Sicherheitsrichtlinien gegen Angriffe

18.1. *System Hacking*
- 18.1.1. Risiken und Schwachstellen
- 18.1.2. Gegenmaßnahmen

18.2. DoS in Dienstleistungen
- 18.2.1. Risiken und Schwachstellen
- 18.2.2. Gegenmaßnahmen

18.3. *Session Hijacking*
- 18.3.1. Der *Hijacking*-Prozess
- 18.3.2. Gegenmaßnahmen zum *Hijacking*

18.4. Umgehung von IDS, Firewalls und Honeypots
- 18.4.1. Ausweichtechniken
- 18.4.2. Implementierung von Gegenmaßnahmen

18.5. *Hacking Web Servers*
- 18.5.1. Angriffe auf Webserver
- 18.5.2. Implementierung von Abwehrmaßnahmen

18.6. *Hacking Web Applications*
- 18.6.1. Angriffe auf Webanwendungen
- 18.6.2. Implementierung von Abwehrmaßnahmen

18.7. *Hacking Wireless Networks*
- 18.7.1. Schwachstellen im Wifi-Netzwerk
- 18.7.2. Implementierung von Abwehrmaßnahmen

18.8. *Hacking Mobile Platforms*
- 18.8.1. Schwachstellen von mobilen Plattformen
- 18.8.2. Implementierung von Gegenmaßnahmen

18.9. *Ransomware*
- 18.9.1. Schwachstellen, die Ransomware verursachen
- 18.9.2. Implementierung von Gegenmaßnahmen

18.10. *Social Engineering*
- 18.10.1. Arten von *Social Engineering*
- 18.10.2. Gegenmaßnahmen für *Social Engineering*

Modul 19. Kryptographie in der IT

19.1. Kryptographie
- 19.1.1. Kryptographie
- 19.1.2. Mathematische Grundlagen

19.2. Kryptologie
- 19.2.1. Kryptologie
- 19.2.2. Kryptoanalyse
- 19.2.3. Steganographie und Stegoanalyse

19.3. Kryptographische Protokolle
- 19.3.1. Grundlegende Blöcke
- 19.3.2. Grundlegende Protokolle
- 19.3.3. Zwischengeschaltete Protokolle
- 19.3.4. Erweiterte Protokolle
- 19.3.5. Exoterische Protokolle

19.4. Kryptographische Techniken
- 19.4.1. Länge des Schlüssels
- 19.4.2. Handhabung der Tasten
- 19.4.3. Arten von Algorithmen
- 19.4.4. Zusammenfassende Funktionen. *Hash*
- 19.4.5. Pseudo-Zufallszahlengeneratoren
- 19.4.6. Verwendung von Algorithmen

19.5. Symmetrische Kryptographie
- 19.5.1. Blockchiffren
- 19.5.2. DES (*Data Encryption Standard*)
- 19.5.3. RC4-Algorithmus
- 19.5.4. AES (*Advanced Encryption Standard*)
- 19.5.5. Kombination von Blockchiffren
- 19.5.6. Ableitung des Schlüssels

19.6. Asymmetrische Kryptographie
- 19.6.1. Diffie-Hellman
- 19.6.2. DSA (*Digital Signature Algorithm*)
- 19.6.3. RSA (Rivest, Shamir und Adleman)
- 19.6.4. Elliptische Kurve
- 19.6.5. Asymmetrische Kryptographie. Typologie

19.7. Digitale Zertifikate
- 19.7.1. Digitale Unterschrift
- 19.7.2. X509-Zertifikate
- 19.7.3. Infrastruktur für öffentliche Schlüssel (PKI)

19.8. Implementierungen
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. *Pretty Good Privacy* (PGP)
- 19.8.4. ISO *Authentication Framework*
- 19.8.5. SSL und TLS
- 19.8.6. Chipkarten als Zahlungsmittel (EMV)
- 19.8.7. Protokolle für Mobiltelefonie
- 19.8.8. *Blockchain*

19.9. Steganographie
- 19.9.1. Steganographie
- 19.9.2. Stegano-Analyse
- 19.9.3. Anwendungen und Einsatzmöglichkeiten

19.10. Quantenkryptographie
- 19.10.1. Quanten-Algorithmen
- 19.10.2. Schutz von Algorithmen vor Quantenberechnungen
- 19.10.3. *Quantum Key Distribution*

Modul 20. Identitäts- und Zugriffsmanagement in der IT-Sicherheit

20.1. Identitäts- und Zugriffsmanagement (IAM)
- 20.1.1. Digitale Identität
- 20.1.2. Identitätsmanagement
- 20.1.3. Identitätsföderation

20.2. Physische Zugangskontrolle
- 20.2.1. Schutzsysteme
- 20.2.2. Bereichssicherheit
- 20.2.3. Wiederherstellungseinrichtungen

20.3. Logische Zugriffskontrolle
- 20.1.1. Authentifizierung: Typologie
- 20.1.2. Authentifizierungsprotokolle
- 20.1.3. Angriffe zur Authentifizierung

20.4. Logische Zugriffskontrolle. MFA-Authentifizierung
- 20.4.1. Logische Zugriffskontrolle. MFA-Authentifizierung
- 20.4.2. Passwörter. Bedeutung
- 20.4.3. Angriffe zur Authentifizierung

20.5. Logische Zugriffskontrolle. Biometrische Authentifizierung
- 20.5.1. Logische Zugriffskontrolle. Biometrische Authentifizierung
  - 20.5.1.1. Biometrische Authentifizierung. Anforderungen
- 20.5.2. Funktionsweise
- 20.5.3. Modelle und Techniken

20.6. Authentifizierungs-Management-Systeme
- 20.6.1. *Single sign on*
- 20.6.2. Kerberos
- 20.6.3. AAA-Systeme

20.7. Authentifizierung-Management-Systeme: AAA-Systeme
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. Kontrollsysteme für den Zugang
- 20.8.1. FW - *Firewalls*
- 20.8.2. VPN - Virtuelle private Netzwerke
- 20.8.3. IDS - *Intrusion Detection System*

20.9. Netzwerk-Zugangskontrollsysteme
- 20.9.1. NAC
- 20.9.2. Architektur und Elemente
- 20.9.3. Betrieb und Standardisierung

20.10. Zugang auf drahtlose Netzwerke
- 20.10.1. Arten von drahtlosen Netzwerken
- 20.10.2. Sicherheit für drahtlose Netzwerke
- 20.10.3. Angriffe auf drahtlose Netzwerke

Modul 21. Sicherheit bei Kommunikation und Softwarebetrieb

21.1. Computersicherheit bei Kommunikation und Softwarebetrieb
- 21.1.1. Computersicherheit
- 21.1.2. Cybersicherheit
- 21.1.3. *Cloud*-Sicherheit

21.2. Computersicherheit in der Kommunikation und im Softwarebetrieb. Typologie
- 21.2.1. Physische Sicherheit
- 21.2.2. Logische Sicherheit

21.3. Sicherheit in der Kommunikation
- 21.3.1. Wichtigste Elemente
- 21.3.2. Netzwerksicherheit
- 21.3.3. *Best Practices*

21.4. Cyberintelligenz
- 21.4.1. *Social Engineering*
- 21.4.2. *Deep Web*
- 21.4.3. *Phishing*
- 21.4.4. *Malware*

21.5. Sichere Entwicklung in Kommunikation und Softwarebetrieb
- 21.1.1. Sichere Entwicklung. HTTP-Protokoll
- 21.1.2. Sichere Entwicklung. Lebenszyklus
- 21.1.3. Sichere Entwicklung. PHP-Sicherheit
- 21.1.4. Sichere Entwicklung. NET-Sicherheit
- 21.1.5. Sichere Entwicklung. *Best Practices*

21.6. Informationssicherheits-Managementsysteme in Kommunikation und Software
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. SIEM-Technologien
- 21.7.1. SIEM-Technologien
- 21.7.2. SOC-Betrieb
- 21.7.3. SIEM *Vendors*

21.8. Die Rolle der Sicherheit in Organisationen
- 21.8.1. Rollen in Organisationen
- 21.8.2. Die Rolle von IoT-Spezialisten in Unternehmen
- 21.8.3. Anerkannte Zertifizierungen auf dem Markt

21.9. Forensische Analyse
- 21.9.1. Forensische Analyse
- 21.9.2. Forensische Analyse. Methodik
- 21.9.3. Forensische Analyse. Tools und Implementierung

21.10. Cybersicherheit heute
- 21.10.1. Große Cyberangriffe
- 21.10.2. Prognosen zur Beschäftigungsfähigkeit
- 21.10.3. Herausforderungen

Modul 22. Sicherheit in *Cloud*-Umgebungen

22.1. Sicherheit in *Cloud Computing*-Umgebungen
- 22.1.1. Sicherheit in *Cloud Computing*-Umgebungen
- 22.1.2. Sicherheit in *Cloud Computing*-Umgebungen. Bedrohungen und Sicherheitsrisiken
- 22.1.3. Sicherheit in *Cloud Computing*-Umgebungen. Wichtige Sicherheitsaspekte

22.2. Arten von *Cloud*-Infrastruktur
- 22.2.1. Öffentlich
- 22.2.2. Privat
- 22.2.3. Hybrid

22.3. Modell der gemeinsamen Verwaltung
- 22.3.1. Vom Anbieter verwaltete Sicherheitselemente
- 22.3.2. Vom Kunden verwaltete Elemente
- 22.3.3. Definition der Sicherheitsstrategie

22.4. Mechanismen der Prävention
- 22.4.1. Authentifizierungs-Management-Systeme
- 22.4.2. Authentifizierungsmanagementsystemen: Zugangspolitik
- 22.4.3. Systeme zur Schlüsselverwaltung

22.5. Sicherung von Systemen
- 22.5.1. Sicherung von Speichersystemen
- 22.5.2. Sicherung von Datenbanksystemen
- 22.5.3. Sichern von Daten bei der Übermittlung

22.6. Schutz der Infrastruktur
- 22.6.1. Entwurf und Implementierung eines sicheren Netzwerks
- 22.6.2. Sicherheit von Computerressourcen
- 22.6.3. Tools und Ressourcen zum Schutz der Infrastruktur

22.7. Erkennung von Bedrohungen und Angriffen
- 22.7.1. *Auditing*-, *Logging*- und Überwachungssysteme
- 22.7.2. Ereignis- und Alarmsysteme
- 22.7.3. SIEM-Systeme

22.8. Reaktion auf Vorfälle
- 22.8.1. Plan zur Reaktion auf Vorfälle
- 22.8.2. Geschäftskontinuität
- 22.8.3. Forensische Analyse und Behebung von Vorfällen der gleichen Art

22.9. Sicherheit in öffentlichen *Clouds*
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. Regulierung und *Compliance*
- 22.10.1. *Compliance* im Bereich Sicherheit
- 22.10.2. Risikomanagement
- 22.10.3. Menschen und Prozesse in Organisationen

Modul 23. Überwachungstools in Sicherheitsrichtlinien für Informationssysteme

23.1. Richtlinien für die Überwachung von Informationssystemen
- 23.1.1. System-Überwachung
- 23.1.2. Metriken
- 23.1.3. Arten von Metriken

23.2. *Auditing* und *Logging* in Systemen
- 23.2.1. *Auditing* und *Logging* in Windows
- 23.2.2. *Auditing* und *Logging* in Linux

23.3. SNMP-Protokoll. *Simple Network Management Protocol*
- 23.3.1. SNMP-Protokoll
- 23.3.2. Betrieb von SNMP
- 23.3.3. SNMP-Tools

23.4. Netzwerküberwachung
- 23.4.1. Netzwerküberwachung in Kontrollsystemen
- 23.4.2. Überwachungstools für Kontrollsysteme

23.5. Nagios. System zur Netzwerküberwachung
- 23.5.1. Nagios
- 23.5.2. Betrieb von Nagios
- 23.5.3. Installation von Nagios

23.6. Zabbix. System zur Netzwerküberwachung
- 23.6.1. Zabbix
- 23.6.2. Betrieb von Zabbix
- 23.6.3. Installation von Zabbix

23.7. Cacti. System zur Netzwerküberwachung
- 23.7.1. Cacti
- 23.7.2. Betrieb von Cacti
- 23.7.3. Installation von Cacti

23.8. Pandora. System zur Netzwerküberwachung
- 23.8.1. Pandora
- 23.8.2. Betrieb von Pandora
- 23.8.3. Installation von Pandora

23.9. SolarWinds. System zur Netzwerküberwachung
- 23.9.1. SolarWinds
- 23.9.2. Betrieb von SolarWinds
- 23.9.3. Installation von SolarWinds

23.10. Regelungen zur Überwachung
- 23.10.1. CIS-Kontrollen zur Prüfung und Registrierung
- 23.10.2. NIST 800-123 (USA)

Modul 24. Sicherheit der Kommunikation von IoT-Geräten

24.1. Von der Telemetrie zum IoT
- 24.1.1. Telemetrie
- 24.1.2. M2M-Konnektivität
- 24.1.3. Demokratisierung der Telemetrie

24.2. IoT-Referenzmodelle
- 24.2.1. IoT-Referenzmodelle
- 24.2.2. Vereinfachte IoT-Architektur

24.3. IoT-Sicherheitsschwachstellen
- 24.3.1. IoT-Geräte
- 24.3.2. IoT-Geräte. Kasuistik der Verwendung
- 24.3.3. IoT-Geräte. Schwachstellen

24.4. IoT-Konnektivität
- 24.4.1. PAN-, LAN-, WAN-Netzwerke
- 24.4.2. Drahtlose Technologien außerhalb des IoT
- 24.4.3. Drahtlose LPWAN-Technologien

24.5. LPWAN-Technologien
- 24.5.1. Das eiserne Dreieck der LPWANs
- 24.5.2. Freie Frequenzbänder vs. Lizensierte Bänder
- 24.5.3. LPWAN-Technologie-Optionen

24.6. LoRaWAN-Technologie
- 24.6.1. LoRaWAN-Technologie
- 24.6.2. LoRaWAN-Anwendungsfälle. Ökosystem
- 24.6.3. LoRaWAN-Sicherheit

24.7. Sigfox-Technologie
- 24.7.1. Sigfox-Technologie
- 24.7.2. Sigfox-Anwendungsfälle. Ökosystem
- 24.7.3. Sicherheit in Sigfox

24.8. IoT-Mobilfunktechnologie
- 24.8.1. IoT-Mobilfunktechnologie (NB-IoT und LTE-M)
- 24.8.2. Anwendungsfälle für IoT-Mobilfunktechnologie Ökosystem
- 24.8.3. IoT-Mobilfunktechnologie-Sicherheit

24.9. WiSUN-Technologie
- 24.9.1. WiSUN-Technologie
- 24.9.2. WiSUN-Anwendungsfälle. Ökosystem
- 24.9.3. Sicherheit in WiSUN

24.10. Andere IoT-Technologien
- 24.10.1. Andere IoT-Technologien
- 24.10.2. Anwendungsfälle und Ökosystem anderer IoT-Technologien
- 24.10.3. Sicherheit in anderen IoT-Technologien

Modul 25. *Business Continuity Plan* in Verbindung mit Sicherheit

25.1. *Business Continuity Plan*
- 25.1.1. Pläne für die Geschäftskontinuität (BCP)
- 25.1.2. Plan für die Geschäftskontinuität (BCP). Schlüsselaspekte
- 25.1.3. *Business Continuity Plan* (BCP) für die Unternehmensbewertung

25.2. Metriken in einem *Business Continuity Plan* (BCP)
- 25.2.1. *Recovery Time Objective* (RTO) und *Recovery Point Objective* (RPO)
- 25.2.2. Maximal verträgliche Zeit (MTD)
- 25.2.3. Mindestanforderungen für die Wiederherstellung (ROL)
- 25.2.4. Wiederherstellungspunkt-Ziel (RPO)

25.3. Kontinuitätsprojekte. Typologie
- 25.3.1. Plan für die Geschäftskontinuität (BCP)
- 25.3.2. IKT-Kontinuitätsplan (ICTCP)
- 25.3.3. Plan zur Wiederherstellung im Katastrophenfall (DRP)

25.4. Risikomanagement im Zusammenhang mit dem BCP
- 25.4.1. Analyse der Auswirkungen auf das Geschäft
- 25.4.2. Vorteile der Implementierung eines BCP
- 25.4.3. Risikobasiertes Denken

25.5. Lebenszyklus eines *Business Continuity Plans*
- 25.5.1. Phase 1: Analyse der Organisation
- 25.5.2. Phase 2: Festlegung der Kontinuitätsstrategie
- 25.5.3. Phase 3: Reaktion auf Notfälle
- 25.5.4. Phase 4: Tests, Wartung und Überprüfung

25.6. Phase der Organisationsanalyse eines BCP
- 25.6.1. Identifizierung der Prozesse, die in den Geltungsbereich des BCP fallen
- 25.6.2. Identifizierung von kritischen Geschäftsbereichen
- 25.6.3. Identifizierung von Abhängigkeiten zwischen Bereichen und Prozessen
- 25.6.4. Bestimmung der geeigneten MTD
- 25.6.5. Liefergegenstände. Erstellung eines Plans

25.7. Phase der Festlegung der Kontinuitätsstrategie in einem BCP
- 25.7.1. Rollen in der Phase der Strategiebestimmung
- 25.7.2. Aufgaben in der Phase der Strategiefestlegung
- 25.7.3. Lieferbare

25.8. Phase der Notfallmaßnahmen eines BCP
- 25.8.1. Rollen in der Reaktionsphase
- 25.8.2. Aufgaben in dieser Phase
- 25.8.3. Lieferbare

25.9. Test-, Wartungs- und Überarbeitungsphase eines BCP
- 25.9.1. Rollen in der Test-, Wartungs- und Überprüfungsphase
- 25.9.2. Aufgaben in der Test-, Wartungs- und Überprüfungsphase
- 25.9.3. Lieferbare

25.10. ISO-Normen im Zusammenhang mit *Business Continuity Plans* (BCP)
- 25.10.1. ISO 22301:2019
- 25.10.2. ISO 22313:2020
- 25.10.3. Andere verwandte ISO- und internationale Normen

Modul 26. Maßnahmen zur praktischen Wiederherstellung nach Sicherheitskatastrophen

26.1. DRP. *Disaster Recovery Plan*
- 26.1.1. Zweck eines DRP
- 26.1.2. Vorteile eines DRP
- 26.1.3. Konsequenzen, wenn Sie keinen DRP haben und diesen nicht auf dem neuesten Stand halten

26.2. Leitfaden für die Definition eines DRP (*Disaster Recovery Plan*)
- 26.2.1. Umfang und Ziele
- 26.2.2. Entwurf der Wiederherstellungsstrategie
- 26.2.3. Zuweisung von Rollen und Verantwortlichkeiten
- 26.2.4. Inventarisierung von Hardware, Software und Diensten
- 26.2.5. Toleranz für Ausfallzeiten und Datenverluste
- 26.2.6. Festlegen der spezifischen Arten von DRPs, die erforderlich sind
- 26.2.7. Umsetzung eines Plans zur Fortbildung, Sensibilisierung und Kommunikation

26.3. Umfang und Ziele eines DRP (*Disaster Recovery Plan*)
- 26.3.1. Sicherstellung der Reaktionsfähigkeit
- 26.3.2. Technologische Komponenten
- 26.3.3. Umfang der Kontinuitätspolitik

26.4. Entwurf einer DRP-Strategie
- 26.4.1. *Disaster-Recovery*-Strategie
- 26.4.2. Budget
- 26.4.3. Personelle und materielle Ressourcen
- 26.4.4. Gefährdete Managementpositionen
- 26.4.5. Technologie
- 26.4.6. Daten

26.5. Kontinuität der Informationsprozesse
- 26.5.1. Planung der Kontinuität
- 26.5.2. Implementierung der Kontinuität
- 26.5.3. Überprüfung der Kontinuitätsbewertung

26.6. Umfang eines BCP (*Business Continuity Plan*)
- 26.6.1. Bestimmung der kritischsten Prozesse
- 26.6.2. Asset-basierter Ansatz
- 26.6.3. Prozessorientierter Ansatz

26.7. Implementierung von gesicherten Geschäftsprozessen
- 26.7.1. Vorrangige Aktivitäten
- 26.7.2. Ideale Wiederherstellungszeiten
- 26.7.3. Überlebensstrategien

26.8. Analyse der Organisation
- 26.8.1. Sammeln von Informationen
- 26.8.2. Analyse der geschäftlichen Auswirkungen
- 26.8.3. Organisatorische Risikoanalyse

26.9. Reaktion auf Notfälle
- 26.9.1. Krisenplan
- 26.9.2. Wiederherstellungspläne für das Betriebsumfeld
- 26.9.3. Verfahren für technische Arbeiten oder Zwischenfälle

26.10. Internationale Norm ISO 27031 BCP
- 26.10.1. Ziele
- 26.10.2. Begriffe und Definitionen
- 26.10.3. Operation

Modul 27. Implementierung von Sicherheitsrichtlinien für die physische und ökologische Sicherheit im Unternehmen

27.1. Sichere Bereiche
- 27.1.1. Physischer Sicherheitsbereich
- 27.1.2. Arbeiten in Sicherheitsbereichen
- 27.1.3. Sicherheit von Büros, Geschäftsräumen und Ressourcen

27.2. Physische Zugangskontrollen
- 27.2.1. Richtlinien zur physischen Zugangskontrolle
- 27.2.2. Physische Zugangskontrollsysteme

27.3. Schwachstellen beim physischen Zugang
- 27.3.1. Die wichtigsten physischen Schwachstellen
- 27.3.2. Umsetzung von Schutzmaßnahmen

27.4. Physiologische biometrische Systeme
- 27.4.1. Fingerabdruck
- 27.4.2. Gesichtserkennung
- 27.4.3. Iris- und Retina-Erkennung
- 27.4.4. Andere physiologische biometrische Systeme

27.5. Verhaltensbiometrische Systeme
- 27.5.1. Erkennung von Unterschriften
- 27.5.2. Erkennung von Schriftzeichen
- 27.5.3. Spracherkennung
- 27.5.4. Andere biometrische Verhaltenssysteme

27.6. Risikomanagement in der Biometrie
- 27.6.1. Implementierung biometrischer Systeme
- 27.6.2. Schwachstellen biometrischer Systeme

27.7. Implementierung von Richtlinien in *Hosts*
- 27.7.1. Installation der Verkabelung, Bereitstellung und Sicherheit
- 27.7.2. Platzierung der Geräte
- 27.7.3. Verlassen der Geräte außerhalb des Gebäudes
- 27.7.4. Unbeaufsichtigte Computerausrüstung und Sicherungspolitik beim Verlassen des Arbeitsplatzes

27.8. Umweltschutz
- 27.8.1. Feuerschutzsysteme
- 27.8.2. Schutzsysteme bei Erdbeben
- 27.8.3. Erdbebenschutzsysteme

27.9. Sicherheit von Datenverarbeitungszentren
- 27.9.1. Sicherheitstüren
- 27.9.2. Videoüberwachungssysteme (CCTV)
- 27.9.3. Sicherheitskontrolle

27.10. Internationale Vorschriften zur physischen Sicherheit
- 27.10.1. IEC 62443-2-1 (europäisch)
- 27.10.2. NERC CIP-005-5 (USA)
- 27.10.3. NERC CIP-014-2 (USA)

Modul 28. Richtlinien für sichere Kommunikation im Unternehmen

28.1. Verwaltung der Netzwerksicherheit
- 28.1.1. Netzwerkkontrolle und -überwachung
- 28.1.2. Netzwerk-Trennung
- 28.1.3. Netzwerk-Sicherheitssysteme

28.2. Sichere Kommunikationsprotokolle
- 28.2.1. TCP/IP-Modell
- 28.2.2. IPSEC-Protokoll
- 28.2.3. TLS-Protokoll

28.3. TLS 1.3-Protokoll
- 28.3.1. Phasen eines TLS 1.3-Prozesses
- 28.3.2. *Handshake*-Protokoll
- 28.3.3. Registrierungsprotokoll
- 28.3.4. Unterschiede zu TLS 1.2

28.4. Kryptographische Algorithmen
- 28.4.1. In der Kommunikation verwendete kryptographische Algorithmen
- 28.4.2. *Cipher-Suites*
- 28.4.3. Erlaubte kryptographische Algorithmen für TLS 1.3

28.5. Digest-Funktionen
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI. Infrastruktur für den öffentlichen Schlüssel
- 28.6.1. PKI und ihre Einrichtungen
- 28.6.2. Digitales Zertifikat
- 28.6.3. Arten von digitalen Zertifikaten

28.7. Tunnel- und Transportkommunikation
- 28.7.1. Tunnelkommunikation
- 28.7.2. Transportkommunikation
- 28.7.3. Verschlüsselte Tunnel-Implementierung

28.8. SSH. *Secure Shell*
- 28.8.1. SSH. Sichere Kapsel
- 28.8.2. Betrieb von SSH
- 28.8.3. SSH-Tools

28.9. Prüfung kryptographischer Systeme
- 28.9.1. Prüfung der Integrität
- 28.9.2. Testen von kryptographischen Systemen

28.10. Kryptografische Systeme
- 28.10.1. Schwachstellen in kryptographischen Systemen
- 28.10.2. Kryptografische Sicherheitsvorkehrungen

Modul 29. Organisatorische Aspekte der Informationssicherheitspolitik

29.1. Interne Organisation
- 29.1.1. Zuweisung von Verantwortlichkeiten
- 29.1.2. Trennung der Aufgaben
- 29.1.3. Kontakte mit Behörden
- 29.1.4. Informationssicherheit in der Projektverwaltung

29.2. Vermögensverwaltung
- 29.2.1. Verantwortung für Vermögenswerte
- 29.2.2. Klassifizierung der Informationen
- 29.2.3. Handhabung von Speichermedien

29.3. Sicherheitspolitiken in Geschäftsprozessen
- 29.3.1. Analyse der anfälligen Geschäftsprozesse
- 29.3.2. Analyse der Auswirkungen auf das Geschäft
- 29.3.3. Einstufung der Prozesse in Bezug auf die geschäftlichen Auswirkungen

29.4. Sicherheitspolitiken in Verbindung mit dem Personalwesen
- 29.4.1. Vor der Einstellung
- 29.4.2. Während der Rekrutierung
- 29.4.3. Beendigung oder Wechsel der Stelle

29.5. Sicherheitsrichtlinien auf Managementebene
- 29.5.1. Managementrichtlinien zur Informationssicherheit
- 29.5.2. BIA - Analyse der Auswirkungen
- 29.5.3. Wiederherstellungsplan als Sicherheitspolitik

29.6. Anschaffung und Wartung von Informationssystemen
- 29.6.1. Anforderungen an die Sicherheit von Informationssystemen
- 29.6.2. Entwicklung und Unterstützung der Datensicherheit
- 29.6.3. Testdaten

29.7. Sicherheit bei Lieferanten
- 29.7.1. IT-Sicherheit mit Zulieferern
- 29.7.2. Management der Bereitstellung des Dienstes mit Garantie
- 29.7.3. Sicherheit der Lieferkette

29.8. Operative Sicherheit
- 29.8.1. Operative Verantwortlichkeiten
- 29.8.2. Schutz vor bösartigem Code
- 29.8.3. Sicherheitskopien
- 29.8.4. Aktivitätsprotokolle und Überwachung

29.9. Sicherheitsmanagement und Vorschriften
- 29.9.1. Einhaltung der gesetzlichen Vorschriften
- 29.9.2. Überprüfung der Informationssicherheit

29.10. Sicherheit im *Business Continuity Management*
- 29.10.1. Kontinuität der Informationssicherheit
- 29.10.2. Redundanzen

Ein kompletter Lehrplan von TECH wird Ihnen beibringen, wie Sie eine visionäre Führungspersönlichkeit werden, die den langfristigen Schutz der Organisation gewährleistet“

04

Lehrziele

Der Weiterbildende Masterstudiengang in Senior Cybersecurity Management (CISO) zielt darauf ab, strategische Führungskräfte fortzubilden, die in der Lage sind, die Informationssicherheit in jeder Art von Organisation zu verwalten. Im Laufe des Programms werden die Teilnehmer Kompetenzen entwickeln, um Cyberrisiken zu erkennen, zu bewerten und abzuschwächen sowie wirksame Sicherheitsrichtlinien umzusetzen. Darüber hinaus erhalten sie ein vertieftes Verständnis für neue Technologien und bewährte Verfahren in der Sicherheitsarchitektur, die den Datenschutz und die Geschäftskontinuität gewährleisten. Das Programm fördert auch eine integrierte geschäftliche Sichtweise der Cybersicherheit, die Initiativen mit den Unternehmenszielen in Einklang bringt und die Einhaltung internationaler Vorschriften gewährleistet. Die Studenten werden darauf vorbereitet, den Wandel voranzutreiben und eine auf den digitalen Schutz ausgerichtete Unternehmenskultur zu fördern.

In dieser 100%igen Online-Spezialisierung finden Sie das aktuellste Lehrmaterial und die aktuellsten Studien in der Universitätsszene“

Allgemeine Ziele

- Fördern strategischer Führungskräfte im Bereich der Cybersicherheit, die in der Lage sind, den Schutz der digitalen Vermögenswerte und technologischen Infrastrukturen globaler Organisationen zu verwalten
- Integrieren der Cybersicherheit in die Unternehmensstrategie, um die Initiativen zum digitalen Schutz mit den allgemeinen Unternehmenszielen in Einklang zu bringen
- Fortbilden in der Umsetzung von Cybersicherheitsrichtlinien und rechtlichen Rahmenbedingungen, die die Einhaltung von Vorschriften und den Informationsschutz in digitalen Umgebungen gewährleisten
- Fördern der Führung und des Managements von Cybersicherheitsteams, um die Fähigkeit zu verbessern, in Krisensituationen strategische Entscheidungen zu treffen und Sicherheitsprojekte auf Organisationsebene zu verwalten

Kommen Sie zu TECH und entwickeln Sie die notwendigen Fähigkeiten, um eine Führungspersönlichkeit zu werden, die Bedrohungen vorhersehen und Chancen nutzen kann“

Spezifische Ziele

Modul 1. Cyberintelligenz und Cybersicherheit

- Entwickeln der erforderlichen Fähigkeiten zur Umsetzung von Strategien für Cyberintelligenz und Cybersicherheit
- Schützen von IT-Systemen vor Cyber-Bedrohungen durch das Sammeln, Analysieren und Nutzen von digitalen Informationen

Modul 2. Host-Sicherheit

- Fortbilden in der Umsetzung von Sicherheitsmaßnahmen auf Hostsystemen
- Schützen von Servern und Geräten vor Schwachstellen, *Malware* und unberechtigtem Zugriff

Modul 3. Netzwerksicherheit (Perimeter)

- Vermitteln der notwendigen Kenntnisse für den Schutz von Computernetzwerken auf Perimeterebene
- Handhaben von Sicherheitstechniken und -werkzeugen wie Firewalls, VPNs und Systemen zur Erkennung von Eindringlingen

Modul 4. Smartphone-Sicherheit

- Vermitteln eines umfassenden Verständnisses für die Sicherheit mobiler Geräte
- Vertiefen Sie den Schutz vor Bedrohungen wie *Malware*, Datenverlust und Angriffen über mobile Anwendungen

Modul 5. IoT-Sicherheit

- Fortbilden der Umsetzung von Sicherheitsrichtlinien für IoT-Geräte
- Schützen der Infrastruktur und der Daten, die von über IoT-Netzwerke und -Plattformen verbundenen Geräten erzeugt werden

Modul 6. Ethisches *Hacking*

- Entwickeln der notwendigen Fähigkeiten zur Durchführung von Penetrationstests und Sicherheitsaudits unter Anwendung von Techniken des ethischen *Hackings*
- In der Lage sein, Schwachstellen zu erkennen und Angriffe zu verhindern

Modul 7. *Reverse Engineering*

- Beherrschen von *Reverse-Engineering*-Techniken, um die Funktionsweise von Software und Hardware zu analysieren und zu verstehen
- Identifizieren potenzieller Schwachstellen und Sicherheitslösungen

Modul 8. Sichere Entwicklung

- Vermitteln von *Best Practices* für die sichere Softwareentwicklung
- Anwenden von Sicherheitsprinzipien während des gesamten Entwicklungszyklus zur Minimierung von Risiken und Schwachstellen in Anwendungen

Modul 9. Praktische Implementierung von Sicherheitsrichtlinien für Software und Hardware

- Vermitteln der erforderlichen Kenntnisse für die Entwicklung und Umsetzung robuster Sicherheitsrichtlinien für Software und Hardware
- Gewährleisten des Schutzes vor internen und externen Bedrohungen

Modul 10. Forensische Analyse

- Entwickeln von Kompetenzen in der digitalen forensischen Analyse
- Untersuchen der Sammlung, Bewahrung und Analyse digitaler Beweise in Fällen von Computersicherheitsvorfällen

Modul 11. Sicherheit in Design und Entwicklung von Systemen
- Berücksichtigen der Integration von Sicherheitsmaßnahmen bereits in der Entwurfs- und Entwicklungsphase von IT-Systemen
- Gewährleisten des Schutzes vor potenziellen Schwachstellen von Beginn des Projekts an

Modul 12. Architekturen und Modelle für die Informationssicherheit
- Bereitstellen der erforderlichen Kenntnisse über Informationssicherheitsarchitekturen und -modelle
- Entwerfen und Implementieren robuster Systeme zum Schutz der Daten und Ressourcen der Organisation

Modul 13. Informationssicherheits-Managementsystem (ISMS)
- Implementieren eines Informationssicherheits-Managementsystems
- Effizientes Schützen von Geschäftsinformationen, um die Einhaltung von Vorschriften und bewährten Verfahren zu gewährleisten

Modul 14. IT-Sicherheitsmanagement
- Vermitteln der notwendigen Kenntnisse, um die Sicherheit der technologischen Infrastrukturen des Unternehmens wirksam zu verwalten
- Minimieren der Risiken und Gewährleisten der betrieblichen Kontinuität

Modul 15. Richtlinien für das Management von Sicherheitsvorfällen
- Fortbilden in der Erstellung und Umsetzung wirksamer Strategien für das Management von Sicherheitsvorfällen
- Erstellen klarer Protokolle für die Erkennung, Analyse und Reaktion auf Sicherheitsverstöße

Modul 16. Risikoanalyse und IT-Sicherheitsumgebung
- Vermitteln der erforderlichen Kenntnisse zur Durchführung einer Risikoanalyse der IT-Umgebung, um Bedrohungen und Schwachstellen zu ermitteln
- Anwenden von Abhilfestrategien zur Sicherung der technologischen Infrastruktur

Modul 17. Sicherheitsrichtlinien für die Analyse von Bedrohungen in Computersystemen
- Fortbilden in der Entwicklung von Sicherheitsrichtlinien, um Bedrohungen für IT-Systeme zu erkennen, zu analysieren und abzuschwächen
- Verwenden geeigneter Tools und Methoden zum Schutz der digitalen Ressourcen der Organisation

Modul 18. Praktische Implementierung von Sicherheitsrichtlinien gegen Angriffe
- Implementieren wirksamer Sicherheitsrichtlinien angesichts möglicher Angriffe
- Gewährleisten des Schutzes von kritischen Systemen und Informationen in der Organisation

Modul 19. Kryptographie in der IT
- Vermitteln der Grundlagen und Anwendungen der Kryptographie im Bereich der Informationstechnologie
- Anwenden von Verschlüsselungs- und Sicherheitsalgorithmen bei der Datenübertragung

Modul 20. Identitäts- und Zugriffsmanagement in der IT-Sicherheit
- Entwickeln Sie die Fähigkeiten, die für die Verwaltung von Identität und Zugang in IT-Systemen erforderlich sind
- Festlegen von Authentifizierungs- und Zugangskontrollrichtlinien zum Schutz der Ressourcen und Daten der Organisation

Modul 21. Sicherheit bei Kommunikation und Softwarebetrieb

- Fortbilden im Bereich des Schutzes der digitalen Kommunikation und der Umsetzung von Sicherheitsmaßnahmen beim Betrieb von Software
- Sicherstellen der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

Modul 22. Sicherheit in *Cloud*-Umgebungen

- Implementieren von Sicherheitsrichtlinien in *Cloud-Computing*-Umgebungen
- Sicherstellen, dass Daten und Anwendungen vor unbefugtem Zugriff und Angriffen geschützt sind

Modul 23. Überwachungstools in Sicherheitsrichtlinien für Informationssysteme

- Fortbilden in der Verwendung von Überwachungsinstrumenten zur Bewertung der Wirksamkeit von Sicherheitsmaßnahmen in Informationssystemen
- Vertiefen der Früherkennung von Schwachstellen und Angriffen

Modul 24. Sicherheit der Kommunikation von IoT-Geräten

- Entwickeln von Kompetenzen für die Umsetzung von Sicherheitsmaßnahmen zum Schutz der Kommunikation zwischen IoT-Geräten
- Minimieren der Risiken, die mit dem Austausch von Daten zwischen verbundenen Geräten einhergehen

Modul 25. *Business Continuity Plan* in Verbindung mit Sicherheit

- Entwickeln eines Plans zur Aufrechterhaltung des Geschäftsbetriebs, um den Schutz und die schnelle Wiederherstellung von Systemen zu gewährleisten
- Festlegen von Protokollen zur Sicherung kritischer Daten im Falle von Sicherheitsvorfällen

Modul 26. Maßnahmen zur praktischen Wiederherstellung nach Sicherheitskatastrophen

- Erstellen von Richtlinien für die Wiederherstellung im Notfall
- Gewährleisten der raschen Wiederherstellung von Systemen und des Schutzes von Daten im Falle größerer Sicherheitsvorfälle

Modul 27. Implementierung von Sicherheitsrichtlinien für die physische und ökologische Sicherheit im Unternehmen

- Fortbilden in der Implementierung von Sicherheitsrichtlinien für die physische und ökologische Sicherheit zum Schutz der physischen Ressourcen der Organisation
- Gewährleisten der richtigen Umgebung für den sicheren Betrieb von Technologiesystemen

Modul 28. Richtlinien für sichere Kommunikation im Unternehmen

- Vermitteln von Kenntnissen zur Entwicklung sicherer Kommunikationsstrategien innerhalb der Organisation
- Schützen von Kommunikationsnetzen und -kanälen vor Spionage und Informationslecks

Modul 29. Organisatorische Aspekte der Informationssicherheitspolitik

- Bereitstellen der erforderlichen Instrumente für die Umsetzung der Unternehmensrichtlinien für das Informationssicherheitsmanagement
- Festlegen geeigneter Rollen, Verantwortlichkeiten und Prozesse zum Schutz von Informationswerten

05

Karrieremöglichkeiten

Nach Abschluss des Weiterbildenden Masterstudiengangs in Senior Cybersecurity Management (CISO) sind die Absolventen umfassend fortgebildet, um Schlüsselrollen beim Schutz und Management der Informationssicherheit in verschiedenen Organisationen zu übernehmen. Sie werden auch in der Lage sein, Sicherheitsstrategien in multinationalen Unternehmen zu leiten und Cyberrisiken zu verwalten und zu mindern. Ebenso werden sie darauf vorbereitet sein, Positionen zu besetzen, die Fähigkeiten zur Leitung von Cybersicherheitsinitiativen und zur Gewährleistung des Schutzes digitaler Werte in jedem Sektor erfordern.

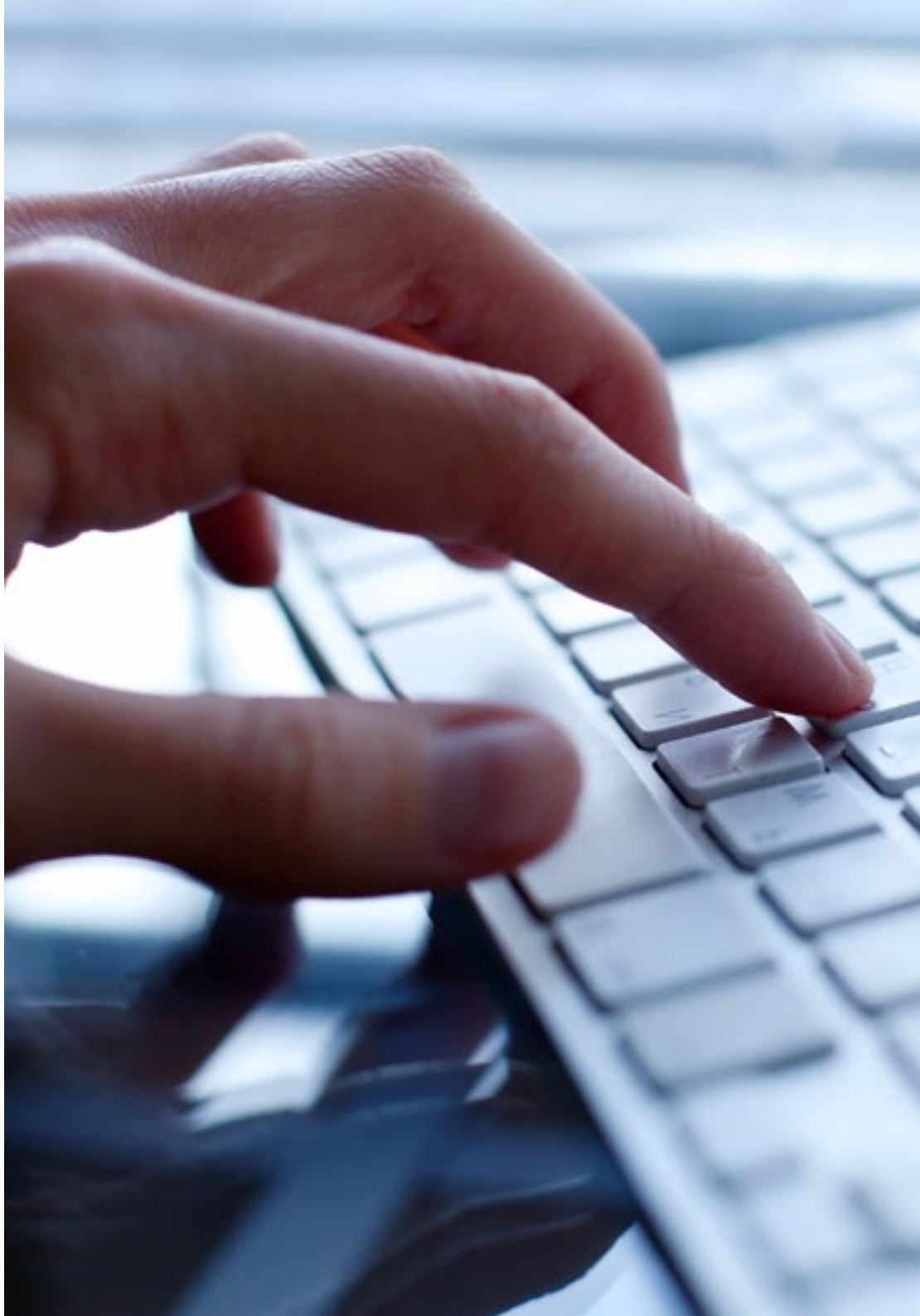
Mit diesem weiterbildenden Masterstudiengang spezialisieren Sie sich als Direktor, der in der Lage ist, Risiken zu antizipieren und kritische Informationen zu schützen“

Profil des Absolventen

Der Absolvent des Weiterbildenden Masterstudiengangs in Senior Cybersecurity Management (CISO) wird eine strategische Führungspersönlichkeit sein, die über ein tiefes Verständnis von Informationssicherheit im Kontext globaler Organisationen verfügt. Er wird in der Lage sein, fortschrittliche Sicherheitsstrategien zu entwerfen und umzusetzen und multidisziplinäre Teams zu leiten. Darüber hinaus wird er über ausgeprägte Management- und Governance-Fähigkeiten verfügen, die ihn in die Lage versetzen, Herausforderungen im Bereich der Cybersicherheit in einer Vielzahl von Sektoren zu bewältigen und den Schutz digitaler Werte zu gewährleisten. Diese Gelegenheit gibt ihm das nötige Rüstzeug an die Hand, um mit den neuesten Technologietrends Schritt zu halten und sich an die sich rasch verändernde digitale Landschaft anzupassen.

> *Bereiten Sie sich darauf vor, zu den besten Fachkräften zu gehören, um die Auswirkungen von Cyberangriffen zu minimieren und schnell wieder zur Normalität zurückzukehren.*

- **Strategische Führung und Anpassungsfähigkeit:** Fähigkeit, multidisziplinäre Teams zu leiten und Sicherheitsrichtlinien zu verwalten und sich an die raschen technologischen und neuen Veränderungen im Bereich der Cybersicherheit anzupassen
- **Risikomanagement und fundierte Entscheidungsfindung:** Fähigkeit, Cyberrisiken zu erkennen, zu bewerten und abzumildern und Entscheidungen auf der Grundlage detaillierter Daten und Analysen zu treffen
- **Kritische Analyse und Management von Vorfällen:** Fähigkeit, Schwachstellen zu erkennen, Sicherheitsvorfälle zu bewältigen und Krisenreaktionen zu koordinieren, um die Geschäftskontinuität zu gewährleisten
- **Effektive Kommunikation und strategisches Denken:** Fähigkeit, Risiken und Lösungen den verschiedenen Interessengruppen klar zu vermitteln und dabei einen ganzheitlichen und strategischen Ansatz für den Schutz digitaler Werte zu verfolgen



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

1. **Chief Information Security Officer (CISO):** Strategische Führungskraft, die für den Informationsschutz und die Cybersicherheit im gesamten Unternehmen verantwortlich ist, Richtlinien entwickelt und die digitale Sicherheitsinfrastruktur beaufsichtigt.
2. **Direktor für Cybersicherheit:** Verantwortlich für die Leitung und Beaufsichtigung der IT-Sicherheitsteams, Entwicklung und Umsetzung von Strategien zum Schutz der technologischen Infrastruktur des Unternehmens.
3. **IT-Sicherheitsbeauftragter:** Verantwortlich für die Verwaltung und Koordinierung der digitalen Sicherheitsrichtlinien, Überwachung des Schutzes von Daten und Computersystemen vor möglichen Bedrohungen.
4. **Berater für Cybersicherheit:** Experte für die Beratung von Unternehmen bei der optimalen Umsetzung und Verwaltung von Cybersicherheitsmaßnahmen, der Risikominderung und der Einhaltung internationaler Vorschriften.
5. **IT-Risikomanager:** Verantwortlich für die Identifizierung, Bewertung und Minderung von Cyberrisiken, die die Sicherheit der Informations- und Technologiesysteme des Unternehmens beeinträchtigen können.
6. **Leiter für Informationssicherheit:** Verantwortlich für die Überwachung und Koordinierung aller Initiativen zum Schutz von Daten und IT-Systemen innerhalb des Unternehmen.

Mit diesem weiterbildenden Masterstudiengang, den nur TECH anbieten kann, sind Sie nur einen Schritt davon entfernt, Ihr Berufsleben zu verbessern“

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.

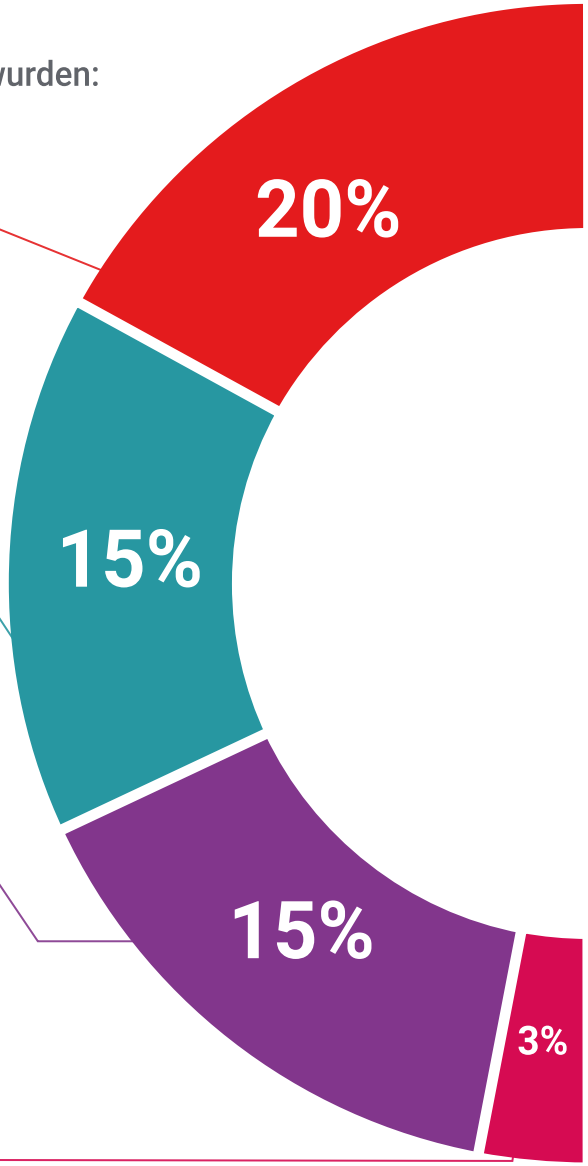
Interaktive Zusammenfassungen

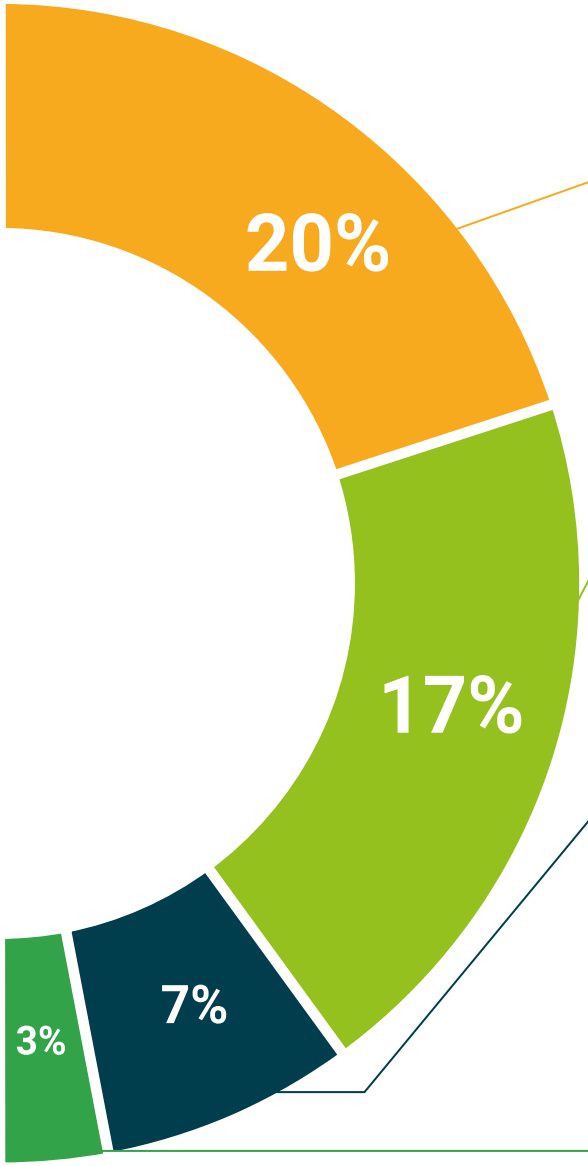
Wir präsentieren die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu festigen.

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 Weiterbildende Masterstudiengang in Senior Cybersecurity Management (CISO, Chief Information Security Officer) verfügt über einen Lehrkörper, der sich aus aktiven Fachleuten zusammensetzt, die den aktuellen Stand in diesem Bereich genau kennen und daher dem Studenten alle Schlüssel zur aktuellen Cybersicherheit vermitteln werden. Auf diese Weise ist gewährleistet, dass der Student dieses Programms die neuesten Fortschritte in diesem Bereich erhält, da er dank des von TECH ausgewählten renommierten Lehrkörpers Zugang zu ihnen hat.

TECH bietet Ihnen die am meisten spezialisierten Direktoren und Lehrkräfte, damit Sie den besten Ansatz und die beste Fortbildung erhalten“

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

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

Hr. Olalla Bonal, Martín

- Senior Manager der *Blockchain*-Praxis bei EY
- Technischer Spezialist für *Blockchain*-Kunden bei IBM
- Direktor für Architektur bei Blocknitive
- Teamkoordinator für nicht relationale verteilte Datenbanken bei wedoIT, Tochtergesellschaft von IBM
- Infrastruktur-Architekt bei Bankia
- Leiter der Layout-Abteilung bei T-Systems
- Abteilungskoordinator für Bing Data España SL

Professoren

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. Entrenas, Alejandro

- Projektleiter für Cybersicherheit, Entelgy Innotec Security
- Berater für Cybersicherheit, Entelgy
- Analyst für Informationssicherheit, Innovery Spanien
- Analyst für Informationssicherheit, Atos
- Hochschulabschluss in Technischem Ingenieurwesen im Bereich Computersysteme an der Universität von Cordoba
- Masterstudiengang in Informationssicherheitsmanagement von der Polytechnischen Universität von Madrid
- ITIL v4 Foundation-Zertifikat für IT-Service-Management, ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced, Avnet
- IBM Security QRadar SIEM 7.1 Foundations, Avnet

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. 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. Gonzalo Alonso, Félix

- CEO und Gründer von Smart REM Solutions
- Leiter der Abteilung Risikotechnik und Innovation bei Dynargy
- Manager und Gründungspartner der Technologieberatung Risknova
- Masterstudiengang in Versicherungsmanagement am Institut für die Zusammenarbeit von Versicherungsgesellschaften
- Hochschulabschluss in Industrietechnik, Spezialisierung auf Industrieelektronik, Päpstliche Universität Comillas

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

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. Nogales Ávila, Javier

- Enterprise Cloud und Sourcing Senior Consultant bei Quint
- Cloud und Technology Consultant bei Indra
- Associate Technology Consultant bei Accenture
- Hochschulabschluss in Industrielle Organisationstechnik an der Universität von Jaén
- MBA in Betriebswirtschaftslehre an der ThePower Business School

Hr. Gómez Rodríguez, Antonio

- Leitender Ingenieur für Cloud-Lösungen bei Oracle
- Mitorganisator des Malaga Developer Meetup
- Beratungsspezialist für die Sopra Group und Everis
- Teamleiter bei System Dynamics
- Software-Entwickler bei SGO Software
- Masterstudiengang in E-Business an der La Salle Wirtschaftsschule
- Aufbaustudiengang in Informationstechnologien und -systemen vom Katalanischen Institut für Technologie
- Hochschulabschluss in Telekommunikationstechnik an der Polytechnischen Universität von Katalonien

Hr. Rodrigo Estébanez, Juan Manuel

- Mitgründer von Ismet Tech
- Manager für Informationssicherheit bei der Ecix-Gruppe
- *Operational Security Officer* bei Atos IT Solutions and Services A/S
- Cybersicherheitsmanagement im Rahmen von Universitätsstudien
- Hochschulabschluss in Ingenieurwesen an der Universität von Valladolid
- Masterstudiengang in Integrierten Managementsystemen an der Universität CEU San Pablo

Hr. Del Valle Arias, Jorge

- Telekommunikationsingenieur mit Erfahrung in der Geschäftsentwicklung
- Smart City Solutions & Software Business Development Manager Spanien, Itron, Inc
- IoT-Berater
- Interim IoT Business Director, TCOMET
- Leiter der Geschäftseinheit IoT, Industrie 4.0, Diode Spanien
- Bereichsleiter für IoT und Telekommunikation, Aicox Soluciones
- Technischer Leiter (CTO) und Leiter der Geschäftsentwicklung, TELYC-Beratung
- Gründer und CEO von Sensor Intelligence
- Leiter der Abteilung Betrieb und Projekte, Codio
- Betriebsleitung bei Codium Networks
- Leitender Hardware- und Firmware-Designer, AITEMIN
- Regionaler Leiter der HF-Planung und -Optimierung - LMDS 3,5-GHz-Netz, Clearwire
- Ingenieur für Telekommunikation von der Polytechnischen Universität von Madrid
- Executive MBA von der International Graduate School von La Salle in Madrid
- Masterstudiengang in Erneuerbare Energien, CEPYME

Hr. Gozalo Fernández, Juan Luis

- Blockchain-basierter Produktmanager für Open Canarias
- Blockchain DevOps Manager bei Alastria
- Direktor für Service Level Technologie bei Santander Spanien
- Manager für die Entwicklung der mobilen Anwendung Tinkerlink bei Cronos Telecom
- Technischer Direktor für IT-Service-Management bei Barclays Bank Spanien
- Hochschulabschluss in Computertechnik an der UNED
- Spezialisierung auf *Deep Learning* bei DeepLearning.ai

Fr. Jurado Jabonero, Lorena

- Leitung der Informationssicherheit (CISO) bei Grupo Pascual
- Cybersecurity Manager bei KPMG, Spanien
- Beraterin für IT-Prozesse und Infrastrukturprojektkontrolle und -management bei Bankia
- Ingenieurin für Verwertungswerkzeuge bei Dalkia
- Entwicklung bei der Banco Popular Gruppe
- Anwendungsentwicklerin von der Polytechnischen Universität von Madrid
- Hochschulabschluss in Computertechnik an der Universität Alfonso X El Sabio
- Technische Ingenieurin in Computer Management von der Polytechnischen Universität von Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) von ISACA

Hr. Ortega Esteban, Octavio

- Spezialist für Marketing und Webentwicklung
- Programmierer für Computeranwendungen und Webentwicklung
- *Chief Operating Officer* bei Smallsquid SL
- Verwalter für E-Commerce bei Ortega y Serrano
- Dozent für Zertifizierungskurse in Computer und Kommunikation
- Dozent für Computersicherheitskurse
- Hochschulabschluss in Psychologie an der Offenen Universität von Katalonien (UOC)
- Höhere Berufsausbildung in *Softwareanalyse*, -design und -lösungen
- Höhere Berufsausbildung in fortgeschrittener Programmierung

Hr. Embid Ruiz, Mario

- Rechtsanwalt mit Spezialisierung auf IKT und Datenschutz bei Martínez-Echevarría Abogados
- Juristischer Leiter von Branddocs SL
- Risikoanalyst im KMU-Segment bei BBVA
- Dozent in universitären Aufbaustudiengängen im Bereich Recht
- Hochschulabschluss in Jura an der Universität Rey Juan Carlos
- Hochschulabschluss in Betriebswirtschaft und Management an der Universität Rey Juan Carlos in Madrid
- Masterstudiengang in Recht der neuen Technologien, Internet und audiovisuelle Medien am Studienzentrum der Universität Villanueva

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 Senior Cybersecurity Management (CISO, Chief Information Security Officer) 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 Senior Cybersecurity Management (CISO, Chief Information Security Officer)** 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 Senior Cybersecurity Management (CISO, Chief Information Security Officer)**

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

Senior Cybersecurity Management
(CISO, Chief Information Security Officer)

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

einzigartiger Code TECH: AFWOR23S techtitute.com/titel


Weiterbildender Masterstudiengang in Senior Cybersecurity Management (CISO, Chief Information Security Officer)

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	ECTS	Kategorie
1°	Cyberintelligenz und Cybersicherheit	103	OB
1°	Host-Sicherheit	103	OB
1°	Netzwerksicherheit (Perimeter)	103	OB
1°	Smartphone-Sicherheit	103	OB
1°	IoT-Sicherheit	103	OB
1°	Ethisches *Hacking*	103	OB
1°	*Reverse Engineering*	103	OB
1°	Sichere Entwicklung	103	OB
1°	Praktische Implementierung von Sicherheitsrichtlinien für Software und Hardware	103	OB
1°	Forensische Analyse	103	OB
1°	Sicherheit in Design und Entwicklung von Systemen	103	OB
1°	Architekturen und Modelle für die Informationssicherheit	103	OB
1°	Informationssicherheits-Managementsystem (ISMS)	103	OB
1°	IT-Sicherheitsmanagement	103	OB
1°	Richtlinien für das Management von Sicherheitsvorfällen	103	OB
2°	Risikoanalyse und IT-Sicherheitsumgebung	103	OB
2°	Sicherheitsrichtlinien für die Analyse von Bedrohungen in Computersystemen	103	OB
2°	Praktische Implementierung von Sicherheitsrichtlinien gegen Angriffe	103	OB
2°	Kryptographie in der IT	103	OB
2°	Identitäts- und Zugriffsmanagement in der IT-Sicherheit	103	OB
2°	Sicherheit bei Kommunikation und Softwarebetrieb	103	OB
2°	Sicherheit in Cloud-Umgebungen	103	OB
2°	Überwachungstools in Sicherheitsrichtlinien für Informationssysteme	103	OB
2°	Sicherheit der Kommunikation von IoT-Geräten	103	OB
2°	*Business Continuity Plan* in Verbindung mit Sicherheit	103	OB
2°	Maßnahmen zur praktischen Wiederherstellung nach Sicherheitskatastrophen	103	OB
2°	Implementierung von Sicherheitsrichtlinien für die physische und ökologische Sicherheit im Unternehmen	103	OB
2°	Richtlinien für sichere Kommunikation im Unternehmen	103	OB
2°	Organisatorische Aspekte der Informationssicherheitspolitik	116	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

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

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

Weiterbildender Masterstudiengang

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

tech technologische universität