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: **24 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: www.techtitute.com/informatik/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-senior-cybersecurity-management-ciso-chief-information-security-officer

Index

01

Präsentation

In der heutigen Welt ist die Cybersicherheit ein grundlegendes Element für Einzelpersonen und Unternehmen, die mehr denn je Angriffen ausgesetzt sind. Dies ist auf die kontinuierliche Entwicklung neuer Technologien und den Digitalisierungsprozess zurückzuführen, der zu Veränderungen in allen Arten von Unternehmen geführt hat und zahlreiche Aktivitäten rationalisiert, aber auch neue Schwachstellen hervorgebracht hat. Aus diesem Grund ist eines der gefragtesten Profile heute das des Cybersecurity Managers, eine wachsende Figur mit zahlreichen beruflichen Möglichkeiten. Der Studiengang befasst sich eingehend mit dieser Figur und bereitet den Informatiker darauf vor, alle aktuellen Herausforderungen in diesem Bereich, in dem auch Managementfähigkeiten und eine unternehmerische Perspektive gefragt sind, wirksam und umfassend zu bewältigen. Darüber hinaus ist der Studiengang zu 100% online konzipiert, so dass er sich perfekt mit der Arbeit vereinbaren lässt und Berufstätige studieren können, wann immer sie wollen.

Dieser Studiengang bereitet Sie auf alle gegenwärtigen und zukünftigen Herausforderungen im Bereich der Cybersicherheit vor und ermöglicht es Ihnen, sich auf das Management in diesem wichtigen Bereich der IT zu spezialisieren"

Bankgeschäfte, Online-Shopping, interne Kommunikation in verschiedenen Organisationen, Verwaltungsabläufe... Heutzutage hat die Digitalisierung die Art und Weise, wie Einzelpersonen und Unternehmen täglich arbeiten, verändert. Sie hat zahlreiche Tätigkeiten rationalisiert, bestimmte Wege überflüssig gemacht, die Lebensqualität der Bevölkerung verbessert und den Unternehmen Kosten gespart. Diese Vorteile haben jedoch auch Nachteile in Bezug auf die Cybersicherheit mit sich gebracht.

Viele der derzeit verwendeten digitalen Technologien und Instrumente werden ständig weiterentwickelt und sind daher angreifbar. Da der Einsatz digitaler Anwendungen und Geräte inzwischen weit verbreitet ist, ist ein Ausfall kritisch, da er die Entwicklung des Unternehmens beeinträchtigen kann, nicht nur in Bezug auf Marketing und Vertrieb, sondern auch in Bezug auf die interne Funktionsweise, die ebenfalls von diesen Hilfsmitteln abhängt.

Aus diesem Grund brauchen die Unternehmen Experten für Cybersicherheit, die auf die verschiedenen Probleme, die in diesem Bereich auftreten können, reagieren können. Eines der gefragtesten Profile ist das des Direktors für Cybersicherheit, eine Position, die eine globale Sicht auf diesen Bereich voraussetzt und auf die dieser weiterbildende Masterstudiengang umfassend vorbereitet. Dieses Programm ist also eine großartige Gelegenheit für Informatiker, da es sie mit den neuesten Entwicklungen in diesem Bereich vertraut macht und sie gleichzeitig auf Managemententscheidungen vorbereitet, die bestes Wissen und Führungsqualitäten erfordern.

All dies basiert auf einer Online-Lernmethodik, die sich an die beruflichen Gegebenheiten der Studenten anpasst, und wird von einem Lehrkörper begleitet, der in diesem Bereich der Informatik großes Ansehen genießt. Außerdem stehen ihnen die besten Bildungstechnologien und die neuesten didaktischen Ressourcen zur Verfügung: interaktive Zusammenfassungen, Videos, Meisterklassen, Fallanalysen und ergänzende Lektüre.

Nicht zu vergessen sind die ergänzenden Materialien zum Lehrplan, wie die 10 Meisterklassen, die von einem international anerkannten Experten für Intelligenz, Cybersicherheit und disruptive Technologien gehalten werden. Dank dieser zusätzlichen Inhalte werden die Absolventen ihre Kenntnisse im Senior Cybersecurity Management (CISO, Chief Information Security Officer) bereichern und ihr Wissen über Konzepte im Zusammenhang mit Cyberintelligenz und Informationssicherheit vertiefen.

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

- Die Entwicklung von Fallstudien, die von IT- und Cybersicherheitsexperten vorgestellt werden
- Die grafischen, schematischen und äußerst praktischen Inhalte sind so konzipiert, dass sie wissenschaftliche und praktische Informationen zu den Disziplinen liefern, die für die berufliche Praxis unerlässlich sind
- Praktische Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens genutzt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden im Cybersicherheitsmanagement
- Theoretische Vorträge, 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

Mit diesem weiterbildenden Masterstudiengang werden Sie in der Lage sein, tiefer in die Bereiche IoT-Sicherheit, Cloud Computing und Blockchain einzusteigen, und Sie werden lernen, wie Sie Audits auf hohem Niveau für alle Arten von Unternehmen und Organisationen durchführen können“

Das Management der Cybersicherheit ist ein wachsendes Berufsprofil, und dieses Programm bietet Ihnen die Möglichkeit, durch die Online-Methodik von TECH die besten Möglichkeiten in diesem Bereich zu nutzen"

Zu den Dozenten gehören Fachleute aus dem Bereich der Cybersicherheit, die ihre Erfahrungen in dieses Programm einbringen, sowie anerkannte Spezialisten aus führenden Unternehmen 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.

Sie werden von einem renommierten Lehrkörper unterstützt, der dafür sorgt, dass Sie alle wichtigen Kenntnisse im Bereich des Cybersecurity-Managements erwerben.

Es stehen Ihnen die neuesten Lehrmittel zur Verfügung, um einen schnellen und effizienten Lernprozess zu gewährleisten.

02

Ziele

Das Hauptziel dieses weiterbildenden Masterstudiengangs ist es, den Informatiker zu einem großen Spezialisten in diesem Bereich zu machen, der ihm den Zugang zu den besten beruflichen Möglichkeiten ermöglicht. Zu diesem Zweck wird er nicht nur die neuesten Entwicklungen im Bereich der Cybersicherheit abdecken, sondern Ihnen auch die besten Werkzeuge an die Hand geben, um eine globale Perspektive der geschäftlichen Anforderungen in diesem Bereich zu erhalten. Auf diese Weise wird er in der Lage sein, die Sicherheit von Unternehmen zu verwalten und die besten Methoden für jeden Fall zu kennen.

Dieser weiterbildende Masterstudiengang wird Ihnen dank seiner umfassenden und aktuellen Inhalte und seines renommierten Lehrkörpers, der sich aus aktiven Cybersecurity-Experten zusammensetzt, helfen, den beruflichen Fortschritt zu erzielen, den Sie anstreben"

Allgemeine Ziele

- Analysieren der Rolle des Cybersecurity-Analysten
- Erforschen des Social Engineering und seiner Methoden
- Untersuchen der Methoden OSINT, HUMINT, OWASP, PTEC, OSSTM, OWISAM
- Durchführen einer Risikoanalyse und Verstehen von Risikokennzahlen
- Bestimmen des angemessenen Einsatzes von Anonymität und der Nutzung von Netzwerken wie TOR, I2P und Freenet
- Zusammenstellen der aktuellen Cybersicherheitsvorschriften
- Generieren von Fachwissen zur Durchführung eines Sicherheitsaudits
- Entwickeln geeigneter Nutzungsrichtlinien
- Prüfen von Erkennungs- und Präventionssystemen für wichtige Bedrohungen
- Bewerten von neuen Systemen zur Erkennung von Bedrohungen und deren Weiterentwicklung gegenüber herkömmlichen Lösungen
- Analysieren der wichtigsten aktuellen mobilen Plattformen, ihrer Funktionen und Nutzung
- Identifizieren, Analysieren und Bewerten der Sicherheitsrisiken von IoT-Projektteilen
- Auswerten der erhaltenen Informationen und Entwickeln von Präventions- und Hacking-Mechanismen
- Anwenden von Reverse Engineering auf die Cybersicherheitsumgebung
- Spezifizieren der Tests, die mit der entwickelten Software durchgeführt werden sollen
- Sammeln aller vorhandenen Beweise und Daten, um einen forensischen Bericht zu erstellen
- Ordnungsgemäßes Erstellen des forensischen Berichts
- Analysieren des aktuellen und zukünftigen Stands der IT-Sicherheit
- Untersuchen der Risiken neu aufkommender Technologien
- Zusammenstellen der verschiedenen Technologien in Bezug auf die Computersicherheit
- Erarbeiten von Fachwissen über ein Informationssystem, die Arten und die zu berücksichtigenden Sicherheitsaspekte
- Identifizieren von Schwachstellen in einem Informationssystem
- Entwickeln der gesetzlichen Bestimmungen und Typisierung von Verbrechen, die ein Informationssystem angreifen
- Bewerten der verschiedenen Sicherheitsarchitekturmodelle, um das für das Unternehmen am besten geeignete Modell zu ermitteln
- Identifizieren der regulatorischen Rahmenbedingungen für die Anwendung und deren Rechtsgrundlagen
- Analysieren der organisatorischen und funktionalen Struktur eines Informationssicherheitsbereichs (das Büro des CISO)
- Analysieren und Entwickeln des Konzepts des Risikos und der Ungewissheit in der Umwelt, in der wir leben
- Prüfen des Risikomanagementmodells auf der Grundlage von ISO 31.000
- Untersuchen der Wissenschaft der Kryptologie und der Beziehung zu ihren Zweigen: Kryptographie, Kryptoanalyse, Steganographie und Stegoanalyse
- Analysieren der Arten von Kryptographie nach der Art des Algorithmus und nach ihrer Verwendung
- Prüfen der digitalen Zertifikate
- Prüfen der Public Key Infrastructure (PKI)
- Entwickeln des Konzepts des Identitätsmanagements
- Identifizieren von Authentifizierungsmethoden
- Generieren von Spezialwissen über das Ökosystem der IT-Sicherheit
- Auswerten von Wissen in Bezug auf Cybersicherheit
- Identifizieren der Sicherheitsbereiche der Cloud
- Analysieren der Dienste und Tools in jedem der Sicherheitsbereiche
- Entwickeln der Sicherheitsspezifikationen für jede LPWAN-Technologie
- Vergleichendes Analysieren der Sicherheit von LPWAN-Technologien

Spezifische Ziele

Modul 1. Cyberintelligenz und Cybersicherheit

- Entwickeln von Methoden für die Cybersicherheit
- Untersuchen des Intelligence-Zyklus und dessen Anwendung auf Cyberintelligenz
- Bestimmen der Rolle des Informationsanalysten und der Hindernisse für Evakuierungsmaßnahmen
- Analysieren von OSINT, OWISAM, OSSTM, PTES, OWASP-Methoden
- Ermitteln der gängigsten Tools für die Nachrichtenproduktion
- Durchführen einer Risikoanalyse und Verstehen der verwendeten Metriken
- Festlegen von Anonymisierungsoptionen und Verwendung von Netzwerken wie TOR, I2P, FreeNet
- Beschreiben im Detail der aktuellen Cybersicherheitsvorschriften

Modul 2. Host-Sicherheit

- Festlegen der Backup-Richtlinien für persönliche und berufliche Daten
- Bewerten der verschiedenen Tools, um Lösungen für bestimmte Sicherheitsprobleme zu finden
- Etablieren von Mechanismen, um das System auf dem neuesten Stand zu halten
- Analysieren der Ausrüstung zur Erkennung von Eindringlingen
- Festlegen der Regeln für den Zugriff auf das System
- Prüfen und Klassifizieren von Mails, um Betrug zu vermeiden
- Erstellen von Listen mit erlaubter Software

Modul 3. Netzwerksicherheit (Perimeter)

- Analysieren der aktuellen Netzwerkarchitekturen, um den zu schützenden Perimeter zu identifizieren
- Entwickeln von spezifischen Firewall- und Linux-Konfigurationen zur Entschärfung der häufigsten Angriffe
- Kompilieren der am häufigsten verwendeten Lösungen wie Snort und Suricata, sowie deren Konfiguration
- Untersuchen der verschiedenen zusätzlichen Schichten, die von Firewalls der neuen Generation und Netzwerkfunktionen in Cloud-Umgebungen bereitgestellt werden
- Bestimmen der Tools für den Netzwerkschutz und Aufzeigen, warum sie für eine mehrschichtige Verteidigung von grundlegender Bedeutung sind

Modul 4. Smartphone-Sicherheit

- Untersuchen der verschiedenen Angriffsvektoren, um zu vermeiden, ein leichtes Ziel zu werden
- Bestimmen der wichtigsten Angriffe und Arten von Malware, denen Benutzer mobiler Geräte ausgesetzt sind
- Analysieren der aktuellsten Geräte, um eine sicherere Konfiguration zu erstellen
- Festlegen der wichtigsten Schritte zur Durchführung eines Penetrationstests auf iOS- und Android-Plattformen
- Entwickeln von Fachwissen über die verschiedenen Schutz- und Sicherheitstools
- Etablieren von Best Practices bei der Programmierung für mobile Geräte

Modul 5. IoT-Sicherheit

- Analysieren der wichtigsten IoT-Architekturen
- Untersuchen von Verbindungstechnologien
- Entwickeln der wichtigsten Anwendungsprotokolle
- Erkennen der verschiedenen Arten von vorhandenen Geräten
- Bewerten der Risikostufen und bekannten Schwachstellen
- Entwickeln von Richtlinien zur sicheren Nutzung
- Festlegen geeigneter Bedingungen für die Verwendung dieser Geräte

Modul 6. Ethisches Hacking

- Prüfen von IOSINT-Methoden
- Sammeln von öffentlich zugänglichen Informationen
- Scannen von Netzwerken nach Informationen im aktiven Modus
- Entwickeln von Testlabors
- Analysieren von Tools für *Pentesting*-Leistungen
- Katalogisieren und Bewerten der verschiedenen Schwachstellen der Systeme
- Konkretisieren der verschiedenen Hacking-Methoden

Modul 7. Reverse Engineering

- Analysieren der Phasen eines Compilers
- Untersuchen der x86-Prozessorarchitektur und der ARM-Prozessorarchitektur
- Bestimmen der verschiedenen Arten von Analysen
- Anwenden von *Sandboxing* in verschiedenen Umgebungen
- Entwickeln verschiedener Techniken zur Analyse von *Malware*
- Entwickeln von Tools für die *Malware*-Analyse

Modul 8. Sichere Entwicklung

- Festlegen der Anforderungen, die für den korrekten Betrieb einer Anwendung auf sichere Weise erforderlich sind
- Überprüfen der Logdateien, um Fehlermeldungen zu verstehen
- Analysieren verschiedener Ereignisse und Entscheidung darüber, was dem Benutzer angezeigt und was in den Logs gespeichert werden soll
- Generieren von bereinigtem, leicht überprüfbarem, qualitativ hochwertigem Code
- Bewerten der geeigneten Dokumentation für jede Phase der Entwicklung
- Konkretisieren des Verhaltens des Servers, um das System zu optimieren
- Entwickeln von modularem, wiederverwendbarem und wartbarem Code

Modul 9. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware

- Bestimmen, was Authentifizierung und Identifizierung ist
- Analysieren der verschiedenen existierenden Authentifizierungsmethoden und ihrer praktischen Umsetzung
- Implementieren der richtigen Zugriffskontrollpolitik für Software und Systeme
- Ermitteln der wichtigsten aktuellen Identifizierungstechnologien
- Generieren von Fachwissen über die verschiedenen Methoden, die für die Absicherung von Systemen existieren

Modul 10. Forensische Analyse

- Identifizieren der verschiedenen Elemente, die ein Verbrechen beweisen
- Generieren von Spezialwissen, um Daten von verschiedenen Medien zu erhalten, bevor sie verloren gehen
- Wiederherstellen von Daten, die absichtlich gelöscht wurden
- Analysieren von Systemlogs und Aufzeichnungen
- Festlegen, wie die Daten dupliziert werden, um die Originale nicht zu verändern
- Untermauern der Beweise für Konsistenz

- Erzeugen eines robusten und nahtlosen Berichts
- Präsentieren von Ergebnissen auf konsistente Weise
- Festlegen, wie der Bericht gegenüber der zuständigen Behörde verteidigt werden soll
- Entwickeln von Strategien für sichere Telearbeit

Modul 11. Sicherheit in Design und Entwicklung von Systemen

- Bewerten der Sicherheit eines Informationssystems über alle seine Komponenten und Schichten hinweg
- Identifizieren aktueller Arten von Sicherheitsbedrohungen und Trends
- Festlegen von Sicherheitsrichtlinien durch Definition von Sicherheits- und Notfallrichtlinien und -plänen
- Analysieren von Strategien und Tools zur Gewährleistung der Integrität und Sicherheit von Informationssystemen
- Anwenden spezifischer Techniken und Tools für jede Art von Angriff oder Sicherheitsschwachstelle
- Schützen der im Informationssystem gespeicherten heiklen Informationen
- Kennen des rechtlichen Rahmens und der Typisierung des Verbrechens, um die Vision mit der Typisierung des Täters und seines Opfers zu vervollständigen

Modul 12. Architekturen und Modelle für die Informationssicherheit

- Abstimmen des Sicherheitsmasterplans auf die strategischen Ziele des Unternehmens
- Einrichten eines kontinuierlichen Risikomanagement-Rahmens als integraler Bestandteil des Master Security Plan
- Festlegen geeigneter Indikatoren für die Überwachung der Umsetzung des ISMS
- Einrichten einer richtlinienbasierten Sicherheitsstrategie
- Analysieren der Ziele und Verfahren im Zusammenhang mit dem Plan zur Sensibilisierung von Mitarbeitern, Lieferanten und Partnern
- Identifizieren der in jeder Organisation geltenden Vorschriften, Zertifizierungen und Gesetze innerhalb des gesetzlichen Rahmens
- Entwickleln der Schlüsselelemente, die in der Norm ISO 27001:2013 gefordert werden
- Implementieren eines Modells zur Verwaltung des Datenschutzes in Übereinstimmung mit der europäischen GDPR/RGPD-Verordnung

Modul 13. Informationssicherheits-Managementsystem (ISMS)

- Analysieren der Vorschriften und Standards, die derzeit für ISMS gelten
- Entwickeln der Phasen, die für die Implementierung eines ISMS in einem Unternehmen erforderlich sind
- Analysieren des Managements von Informationssicherheitsvorfällen und der Implementierungsverfahren

Modul 14. IT-Sicherheitsmanagement

- Identifizieren der verschiedenen Strukturen, die ein Bereich der Informationssicherheit haben kann
- Entwickeln eines Sicherheitsmodells, das auf drei Verteidigungslinien basiert
- Vorstellen der verschiedenen periodischen und außerordentlichen Ausschüsse, in denen der Bereich Cybersicherheit vertreten ist
- Bestimmen der technologischen Hilfsmittel, die die Hauptfunktionen des Security Operations Team (SOT) unterstützen
- Bewerten der für jedes Szenario geeigneten Maßnahmen zur Kontrolle der Schwachstellen
- Entwickeln des Rahmenwerks für Sicherheitsoperationen auf der Grundlage des NIST CSF
- Festlegen des Umfangs der verschiedenen Arten von Audits (*Red Team, Pentesting, Bug Bounty* usw.)

- Vorschlagen von Aktivitäten nach einem Sicherheitsvorfall
- Einrichten einer Kommandozentrale für Informationssicherheit, die alle relevanten Akteure (Behörden, Kunden, Lieferanten usw.) einbezieht

Modul 15. Richtlinien für das Management von Sicherheitsvorfällen

- Entwickeln von Fachwissen über den Umgang mit Vorfällen, die durch Computersicherheitsereignisse verursacht werden
- Festlegen der Arbeitsweise eines Teams zur Bearbeitung von Sicherheitsvorfällen
- Analysieren der verschiedenen Phasen des Managements von IT-Sicherheitsvorfällen
- Untersuchen der standardisierten Protokolle für den Umgang mit Sicherheitsvorfällen

Modul 16. Risikoanalyse und IT-Sicherheitsumgebung

- Untersuchen des Umfelds, in dem wir tätig sind, mit einem ganzheitlichen Blick
- Identifizieren der wichtigsten Risiken und Potenziale, die das Erreichen unserer Ziele beeinträchtigen können
- Analysieren der Risiken auf der Grundlage der besten uns zur Verfügung stehenden Methoden
- Bewerten der potenziellen Auswirkungen dieser Risiken und Chancen
- Entwickeln von Techniken, um die Risiken und Potenziale so anzugehen, dass der Mehrwert maximiert wird
- Vertiefen der verschiedenen Techniken zur Übertragung von Risiko und Wert
- Erzielen von Mehrwert durch die Entwicklung eigener Modelle für ein agiles Risikomanagement
- Prüfen der Ergebnisse, um kontinuierliche Verbesserungen im Projekt- und Prozessmanagement auf der Grundlage risikoorientierter oder Risk-Driven Managementmodelle vorzuschlagen
- Innovieren und Umwandeln allgemeiner Daten in relevante Informationen für die risikobasierte Entscheidungsfindung

Modul 17. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

- Analysieren der Bedeutung von Bedrohungen
- Bestimmen der Phasen des präventiven Bedrohungsmanagements
- Vergleichen verschiedener Methoden des Bedrohungsmanagements

Modul 18. Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

- Bestimmen der verschiedenen realen Angriffe auf unser Informationssystem
- Bewerten der verschiedenen Sicherheitsmaßnahmen zur Eindämmung von Angriffen
- Implementieren der technischen Maßnahmen zur Abschwächung der wichtigsten Bedrohungen

Modul 19. Kryptographie in der IT

- Zusammenstellen der grundlegenden Operationen (XOR, große Zahlen, Substitution und Transposition) und der verschiedenen Komponenten (One-Way-Funktionen, Hash, Zufallszahlengeneratoren)
- Analysieren kryptographischer Techniken
- Entwickeln verschiedener kryptographische Algorithmen
- Demonstrieren der Verwendung digitaler Signaturen und ihrer Anwendung in digitalen Zertifikaten
- Bewerten von Schlüsselverwaltungssystemen und der Bedeutung von kryptographischen Schlüssellängen
- Untersuchen von Algorithmen zur Schlüsselableitung
- Analysieren des Lebenszyklus von Schlüsseln
- Auswerten von Blockchiffre- und Stromchiffre-Modi
- Bestimmen der Pseudo-Zufallszahlengeneratoren
- Entwickeln realer Kryptographie-Anwendungen, wie Kerberos, PGP oder Smart Cards

- Prüfen verwandter Verbände und Gremien, wie ISO, NIST oder NCSC
- Bestimmen der Herausforderungen in der Kryptographie des Quantencomputings

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

- Entwickeln des Konzepts der digitalen Identität
- Bewerten der physischen Zugangskontrolle zu formationssicherheit
- Grundlagen der biometrischen Authentifizierung und MFA-Authentifizierung
- Bewerten von Angriffen auf die Vertraulichkeit von Informationen
- Analysieren des Identitätsverbundes
- Einrichten der Netzwerkzugangskontrolle

Modul 21. Sicherheit bei Kommunikation und Softwarebetrieb

- Entwickeln von Fachwissen über physische und logische Sicherheit
- Demonstrieren von Kenntnissen über Kommunikation und Netzwerke
- Identifizieren größerer bösartiger Angriffe
- Einrichten eines sicheren Entwicklungsrahmen
- Nachweisen von Kenntnissen über die wichtigsten Vorschriften zum Management von Informationssicherheitssystemen
- Begründen des Betriebs eines operativen Zentrums für Cybersicherheit
- Demonstrieren der Bedeutung von Cybersicherheitspraktiken für organisatorische Katastrophen

Modul 22. Sicherheit in Cloud-Umgebungen

- Identifizieren der Risiken bei der Bereitstellung einer öffentlichen Cloud-Infrastruktur
- Definieren der Sicherheitsanforderungen
- Entwickeln eines Sicherheitsplans für eine Cloud-Bereitstellung
- Identifizieren der Cloud-Dienste, die für die Ausführung eines Sicherheitsplans eingesetzt werden sollen
- Bestimmen der operativen Anforderungen für Präventionsmechanismen
- Festlegen von Leitlinien für ein Logging- und Überwachungssystem
- Vorschlagen von Maßnahmen zur Reaktion auf Vorfälle

Modul 23. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

- Entwickeln des Konzepts der Überwachung und Implementierung von Metriken
- Konfigurieren von Audit-Trails auf Systemen und Überwachungsnetzwerken
- Zusammenstellen der besten Systemüberwachungstools, die derzeit auf dem Markt sind

Modul 24. Sicherheit der Kommunikation von IoT-Geräten

- Einführen in die vereinfachte IoT-Architektur
- Erklären der Unterschiede zwischen allgemeinen Konnektivitätstechnologien und Konnektivitätstechnologien für das IoT
- Etablieren des Konzepts des Eisernen Dreiecks der IoT-Konnektivität
- Analysieren der Sicherheitsspezifikationen der LoRaWAN-Technologie, NB-IoT-Technologie und WiSUN-Technologie
- Begründen der Wahl der richtigen IoT-Technologie für jedes Projekt

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

- Vorstellen der wichtigsten Elemente jeder Phase und Analysieren der Merkmale des *Business Continuity Plan* (BCP)
- Begründen der Notwendigkeit eines *Business Continuity Plans*
- Bestimmen der Erfolgs- und Risikokarten für jede Phase des *Business Continuity Plans*
- Festlegen eines Aktionsplans für die Umsetzung
- Bewerten der Vollständigkeit eines *Business Continuity Plans* (BCP)
- Entwickeln eines erfolgreichen Implementierungsplan für einen *Business Continuity Plan*

Modul 26. Praktische Sicherheitsrichtlinien für die Wiederherstellung im Katastrophenfall

- Generieren von Fachwissen über das Konzept der Kontinuität der Informationssicherheit
- Entwickeln eines Business Continuity Plans
- Analysieren eines IKT-Kontinuitätsplans
- Entwerfen eines Wiederherstellungsplans für den Katastrophenfall

Modul 27. Implementierung von physischen und ökologischen Sicherheitspolitiken im Unternehmen

- Analysieren der Begriffe sicherer Bereich und sicherer Umkreis
- Untersuchen der Biometrie und biometrischer Systeme
- Umsetzen der richtigen Sicherheitsrichtlinien für die physische Sicherheit
- Entwickeln der geltenden Vorschriften für sichere Bereiche von Computersystemen

Modul 28. Richtlinien für sichere Kommunikation im Unternehmen

- Sichern eines Kommunikationsnetzwerks durch Partitionierung des Netzwerks
- Analysieren der verschiedenen Verschlüsselungsalgorithmen, die in Kommunikationsnetzwerken verwendet werden
- Implementieren verschiedener Verschlüsselungstechniken im Netzwerk wie TLS, VPN oder SSH

Modul 29. Organisatorische Aspekte der Informationssicherheitspolitik

- Implementieren eines ISMS im Unternehmen
- Bestimmen, welche Abteilungen die Implementierung des Sicherheitsmanagementsystems abdecken soll
- Implementieren der notwendigen Sicherheitsmaßnahmen im Betrieb

Dieser weiterbildende Masterstudiengang bringt Sie in Ihrer Karriere als Cybersecurity-Spezialist einen Schritt weiter und vermittelt Ihnen alles, was Sie brauchen, um sich an das komplexe IT-Umfeld von heute anzupassen"

03

Kompetenzen

Während dieses weiterbildenden Masterstudiengangs erwirbt die Fachkraft eine Reihe von Instrumenten und Kompetenzen, die sie in die Lage versetzt, im Cybersecurity-Management eines Großunternehmens zu arbeiten. Aus diesem Grund konzentriert sich dieses Programm nicht nur auf IT-Aspekte, sondern berücksichtigt auch den Digitalisierungsprozess, aufkommende Technologien und wie sich diese Elemente auf die allgemeinen und täglichen Aktivitäten von Organisationen auswirken. Auf diese Weise wird der Absolvent in der Lage sein, sich an den aktuellen Kontext anzupassen und die besten Sicherheitslösungen für jedes Unternehmen zu kennen.

Verbessern Sie Ihre Fähigkeiten, um der große Spezialist für Cybersicherheit in Ihrem Umfeld zu werden"

Allgemeine Kompetenzen

- Kennen der Methoden, die im Bereich der Cybersicherheit verwendet werden
- Wissen, wie man jede Art von Bedrohung bewertet, um in jedem Fall eine optimale Lösung anzubieten
- In der Lage sein, intelligente Komplettlösungen zu erstellen, um das Verhalten bei Zwischenfällen zu automatisieren
- Wissen, wie man die Risiken im Zusammenhang mit Schwachstellen innerhalb und außerhalb des Unternehmens einschätzen kann
- Verstehen der Entwicklung und der Auswirkungen des IoT im Laufe der Zeit
- Nachweisen, dass ein System verwundbar ist, es zu Präventionszwecken angreifen und solche Probleme lösen können
- Wissen, wie man Sandboxing in verschiedenen Umgebungen anwendet
- Kennen der Richtlinien, die ein guter Entwickler befolgen muss, um die notwendige Sicherheit zu gewährleisten
- Anwenden der am besten geeigneten Sicherheitsmaßnahmen in Abhängigkeit von den Bedrohungen
- Festlegen der Sicherheitspolitik und des Sicherheitsplans eines Unternehmens für Informationssysteme und Vervollständigung des Entwurfs und der Umsetzung des Notfallplans
- Erstellen eines Audit-Programms, das den Selbstbewertungsbedarf der Organisation in Bezug auf die Cybersicherheit abdeckt
- Entwickeln eines Programms zum Scannen und Überwachen von Schwachstellen und eines Plans zur Reaktion auf Cyber-Sicherheitsvorfälle
- Maximieren der sich bietenden Chancen und Eliminierung aller potenziellen Risiken durch Design
- Zusammenstellen der Schlüsselverwaltungssysteme
- Bewerten der Informationssicherheit eines Unternehmens
- Analysieren der Systeme für den Informationszugang
- Entwickeln von Best Practices für die sichere Entwicklung
- Darstellen der Risiken, die Unternehmen eingehen, wenn sie nicht über eine sichere Informationssicherheitsumgebung verfügen

Dieses Programm wird Sie in die Zukunft der Cybersicherheit führen"

Spezifische Kompetenzen

- Wissen, wie man defensive Sicherheitsmaßnahmen durchführt
- Verfügen über ein tiefgehendes und spezialisiertes Verständnis von Cybersicherheit
- Verfügen über spezielle Kenntnisse auf dem Gebiet der Cybersicherheit und Cyber Intelligence
- Verfügen über fundierte Kenntnisse grundlegender Aspekte, wie z. B. des Informationszyklus, der Informationsquellen, des Social Engineering, der OSINT-Methodik, des HUMINT, der Anonymisierung, der Risikoanalyse, der bestehenden Methoden (OWASP, OWISAM, OSSTM, PTES) und der bestehenden Cybersicherheitsvorschriften
- Verstehen der Bedeutung einer mehrschichtigen Verteidigung, auch bekannt als Defense in Depth, die alle Aspekte eines Unternehmensnetzwerks abdeckt, wobei einige der besprochenen Konzepte und Systeme auch gestärkt und Umgebung genutzt und angewendet werden können
- Wissen, wie man Sicherheitsverfahren für Smartphones und tragbare Geräte anwendet
- Kennen der Mittel des sogenannten ethischen Hackings und Schutz eines Unternehmens vor einer Cyber-Attacke
- In der Lage sein, einen Cybersicherheitsvorfall zu untersuchen
- Kennen der verschiedenen verfügbaren Angriffs- und Verteidigungstechniken
- Analysieren der Rolle des Chief Information Security Officer (CISO)
- Verstehen der Funktionsweise von Social Engineering und seiner Methoden
- Entwickeln eines Informationssicherheits-Managementsystems (ISMS)
- Identifizieren der Schlüsselelemente, aus denen ein ISMS besteht
- Anwenden der MAGERIT-Methodik, um das Modell weiterzuentwickeln und einen Schritt weiter zu gehen
- Entwickeln neuer Risikomanagement-Methoden auf der Grundlage des Konzepts des Agile Risk Management
- Identifizieren, Analysieren, Bewerten und Behandeln der Risiken, mit denen die Fachleute konfrontiert sind, aus einer neuen Geschäftsperspektive auf der Grundlage eines Risk-Driven oder risikoorientierten Modells, das es nicht nur ermöglicht, in seinem eigenen Umfeld zu überleben, sondern auch seinen eigenen Wertbeitrag zu steigern
- Untersuchen des Prozesses der Entwicklung einer Sicherheitsstrategie bei der Bereitstellung von Cloud-Diensten für Unternehmen
- Bewerten der Unterschiede in den spezifischen Implementierungen der verschiedenen Public Cloud-Anbieter
- Bewerten der IoT-Konnektivitätsoptionen für ein Projekt, mit Schwerpunkt auf LPWAN-Technologien
- Einführen in die grundlegenden Spezifikationen der wichtigsten LPWAN-Technologien für das IoT

04

Kursleitung

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.

Schreiben Sie sich ein und erhalten Sie Zugang zu den fortschrittlichsten Kenntnissen in diesem Bereich, die von Fachleuten mit umfassender Erfahrung auf dem Gebiet der Cybersicherheit vermittelt werden"

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 Praxis und Fakultätsleiter der MPS-Programme für **Angewandte Intelligenz, Risikomanagement für Cybersicherheit, Technologiemanagement und Informationstechnologiemanagement** an der **Universität von Georgetown.**

Dr. Lemieux, Frederic

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

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

Leitung

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical Hacking, Nationales Referenzzentrum für IT und Telekommunikation in Getafe, Madrid
- Zertifizierte E-Council-Ausbilderin, Madrid
- 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 Offizieller EC-Council und CompTIA von der Fachhochschule für neue Technologien CICE

Hr. Catalá Barba, José Francisco

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

Hr. 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. Peralta Alonso, Jon

- Senior Consultant - Datenschutz und Cybersicherheit
- Jurist / Rechtsberater bei Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Rechtsberate / 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. von Kastilien
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht,

Hr. Redondo, Jesús Serrano

- Webentwickler und Cybersecurity-Techniker
- Web-Entwickler bei Roams, Palencia
- FrontEnd-Entwickler bei Telefónica, Madrid
- FrontEnd-Entwickler bei Best Pro Consulting SL, Madrid
- Installateur für Telekommunikationseinrichtungen und -dienste bei Grupo Zener, Castilla y León
- Installateur für Telekommunikationsanlagen und -dienste bei Lican Comunicaciones SL, Castilla y León
- Zertifikat in Computersicherheit, CFTIC Getafe, Madrid

- Höherer Techniker für Telekommunikations- und Computersysteme vom IES Trinidad
  Arroyo, Palencia
- Höherer Techniker 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, Katalanisches Institut für Technologie
- Hochschulabschluss in Telekommunikationstechnik an der Polytechnischen Universität von Katalonien

Hr. Gonzalo Alonso, Félix

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

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. 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

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. Entrenas, Alejandro

- Projektleiter für Cybersicherheit
- Projektleiter für Cybersicherheit, Entelgy Innotec Security
- Berater für Cybersicherheit, Entelgy
- Analyst für Informationssicherheit, Innovery Spanien
- Analyst für Informationssicherheit, Atos
- Hochschulabschluss als Ingenieur für Computersysteme an der Universität von Cordoba
- Masterstudiengang in Informationssicherheitsmanagement an der Polytechnischen Universität 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. Ortega Esteban, Octavio

- Spezialist für Marketing und Webentwicklung
- Freiberuflicher Computeranwendungsprogrammierer und Webentwickler
- *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)
- Höherer Techniker in Softwareanalyse, -design und -lösungen
- Höherer Universitätstechniker in fortgeschrittener Programmierung

05

Struktur und Inhalt

Dieser Weiterbildende Masterstudiengang in Senior Cybersecurity Management (CISO, Chief Information Security Officer) besteht aus 20 Modulen und wurde sorgfältig konzipiert, um Fachleuten die neuesten Entwicklungen in diesem Bereich näher zu bringen. So lernen Sie die neuesten Fortschritte in Bereichen wie Smartphone-Sicherheit, Sicherheit im Internet der Dinge, sichere Entwicklung, Kryptographie und Sicherheit in Cloud-Computing-Umgebungen kennen. Mit diesem Lehrplan erhält der Informatiker also Zugang zu den aktuellsten und vollständigsten Kenntnissen, die ihn schnell zu einem hoch angesehenen Cybersicherheitsspezialisten machen.

Sie werden keinen umfassenderen Inhalt als diesen finden, um auf dem Gebiet der Cybersicherheit auf dem neuesten Stand zu sein"

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. IT-Sicherheitsprüfung
- 1.5.2. Dokumentation und Berechtigungen für Audits
- 1.5.3. Arten von Audits
- 1.5.4. Liefergegenstände
  - 1.5.4.1. Technischer Bericht
  - 1.5.4.2. Exekutivbericht

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*-Standards
- 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. Sicherungskopien
- 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. HIDS Eindringlingsdetektoren
- 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 - *Endpunkt-Erkennung und Reaktion*
- 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. Repositories 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. Block*Hosts* und Deny*Hosts*
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. Whitelisting und Blacklisting
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
4.1. Informationsstände
4.2. Datenschutz und Vertraulichkeit

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. Nicht erzwungener Benutzer
4.6.2. *Malware*
4.6.2.1. Arten von *Malware*
4.6.3. Social Engineering
4.6.4. Datenleck
4.6.5. Informationsdiebstahl
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. Ausführung der Payload und Extraktion von 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. Tools
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 des 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 Umsetzung von Sicherheitspolitiken für Software und Hardware

9.1. Praktische Umsetzung von Sicherheitspolitiken 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. Sicherungskopien
- 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. Systeminformation
  - 10.1.1.2. Netzwerkinformation
  - 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 Anti-Forensik-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. Forensische Analyse von Windows
- 10.3.2. Forensische Analyse von Linux
- 10.3.3. Forensische Analyse Mac

10.4. Forensische Netzwerkanalyse
- 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. Forensische Webanalyse
- 10.5.1. Untersuchung von Webangriffen
- 10.5.2. Angriffserkennung
- 10.5.3. Standort der IP-Adresse

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

10.7. Forensische Cloud-Analyse
- 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 forensischen *Cloud*-Analyse
- 10.7.3. Untersuchung von *Cloud*-Speicherdiensten
- 10.7.4. Forensische Analysetools 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. Forensische Handy-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

1.2. 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: Etappen
- 11.2.4. Methoden von Informationssystemen

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 eines Informationssystems. Sicherheitsprotokolle
- 11.4.1. Sicherheit eines Informationssystems
  - 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 eines Informationssystems

11.5. Sicherheit eines Informationssystems. 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. Typen
- 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 Information
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 DSB. Funktionen

Modul 13. Informationssicherheits-Managementsystem (ISMS)

13.1. Sicherheit der Information. Schlüsselaspekte
13.1.1. Sicherheit der Information
13.1.1.1. Vertraulichkeit
13.1.1.2. Integrität
13.1.1.3. Verfügbarkeit
13.1.1.4. Maßnahmen der Informationssicherheit
13.2. Informationssicherheits-Managementsystem
13.2.1. Informationssicherheits-Managementsystem
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 27.000-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 allgemeinen Informationssicherheitssystems
- 13.7.4. Richtlinien des allgemeinen Informationssicherheitssystems
- 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
- 14.10.1. 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 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. Methodik NIST
  - 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 der Datenerhebung
- 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. Werkzeuge für Intrusion Detection und Prevention Systeme (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. CCN-STIC Sicherheitsleitfaden 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 Computersicherheitsvorfälle
- 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. Wirtschaft
16.1.2.3. Sozial
16.1.2.4. Technologisch
16.1.2.5. Ökologisch/Umweltbezogen
16.1.2.6. Legal
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. ISO 31.000:2018 Richtlinien zum Risikomanagement
16.3.1. Objekt
16.3.2. Grundsätze
16.3.3. Referenzrahmen
16.3.4. Prozesse
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 Cyber-Risiken
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. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

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 Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

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. Authentifizierung MFA
- 20.4.1. Logische Zugriffskontrolle. Authentifizierung MFA
- 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 in der Kommunikation und im 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. Bewährte Praktiken

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. Bewährte Praktiken

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. Cybersecurity 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. Öffentliches
- 22.2.2. Öffentlich
- 22.2.3. Privat

22.3. Hybrid
- 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. Überwachungswerkzeuge in Sicherheitspolitiken 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. Netzwerk-Überwachung
- 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 einer BCP
- 25.7.1. Rollen in der Phase der Strategiebestimmung
- 25.7.2. Aufgaben in der Phase der Strategiefestlegung
- 25.7.3. Liefergegenstände

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

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. Liefergegenstände

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. Praktische Sicherheitspolitiken für die Notfallwiederherstellung

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 (Disaster Recovery)
- 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 (PA)
- 26.7.2. Ideale Wiederherstellungszeiten (IRT)
- 26.7.3. Überlebensstrategien

26.8. Analyse der Organisation
- 26.8.1. Sammeln von Informationen
- 26.8.2. Analyse der geschäftlichen Auswirkungen (BIA)
- 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 physischen und ökologischen Sicherheitspolitiken 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 TLS1.3-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. Tunnel-Kommunikation
- 28.7.2. Transport-Kommunikation
- 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 Information
- 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. Sicherungskopien
- 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

Sie werden in der Lage sein, Themen wie den Business-Continuity-Plan im Zusammenhang mit Sicherheit oder Identitäts- und Zugangsmanagement in der IT-Sicherheit zu vertiefen"

06

Methodik

Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: ***das Relearning***.
Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem ***New England Journal of Medicine*** als eines der effektivsten angesehen.

Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen hinter sich lässt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"

Fallstudie zur Kontextualisierung aller Inhalte

Unser Programm bietet eine revolutionäre Methode zur Entwicklung von Fähigkeiten und Kenntnissen. Unser Ziel ist es, Kompetenzen in einem sich wandelnden, wettbewerbsorientierten und sehr anspruchsvollen Umfeld zu stärken.

Mit TECH werden Sie eine Art des Lernens erleben, die an den Grundlagen der traditionellen Universitäten auf der ganzen Welt rüttelt"

Sie werden Zugang zu einem Lernsystem haben, das auf Wiederholung basiert, mit natürlichem und progressivem Unterricht während des gesamten Lehrplans.

Der Student wird durch gemeinschaftliche Aktivitäten und reale Fälle lernen, wie man komplexe Situationen in realen Geschäftsumgebungen löst.

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist ein von Grund auf neu entwickeltes, intensives Lehrprogramm, das die anspruchsvollsten Herausforderungen und Entscheidungen in diesem Bereich sowohl auf nationaler als auch auf internationaler Ebene vorsieht. Dank dieser Methodik wird das persönliche und berufliche Wachstum gefördert und ein entscheidender Schritt in Richtung Erfolg gemacht. Die Fallmethode, die Technik, die diesem Inhalt zugrunde liegt, gewährleistet, dass die aktuellste wirtschaftliche, soziale und berufliche Realität berücksichtigt wird.

> *Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Informatikschulen der Welt, seit es sie gibt. Die Fallmethode wurde 1912 entwickelt, damit Jurastudenten das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernen. Sie bestand darin, ihnen reale komplexe Situationen zu präsentieren, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen konnten, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

Was sollte eine Fachkraft in einer bestimmten Situation tun? Mit dieser Frage konfrontieren wir Sie in der Fallmethode, einer handlungsorientierten Lernmethode. Während des gesamten Kurses werden die Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

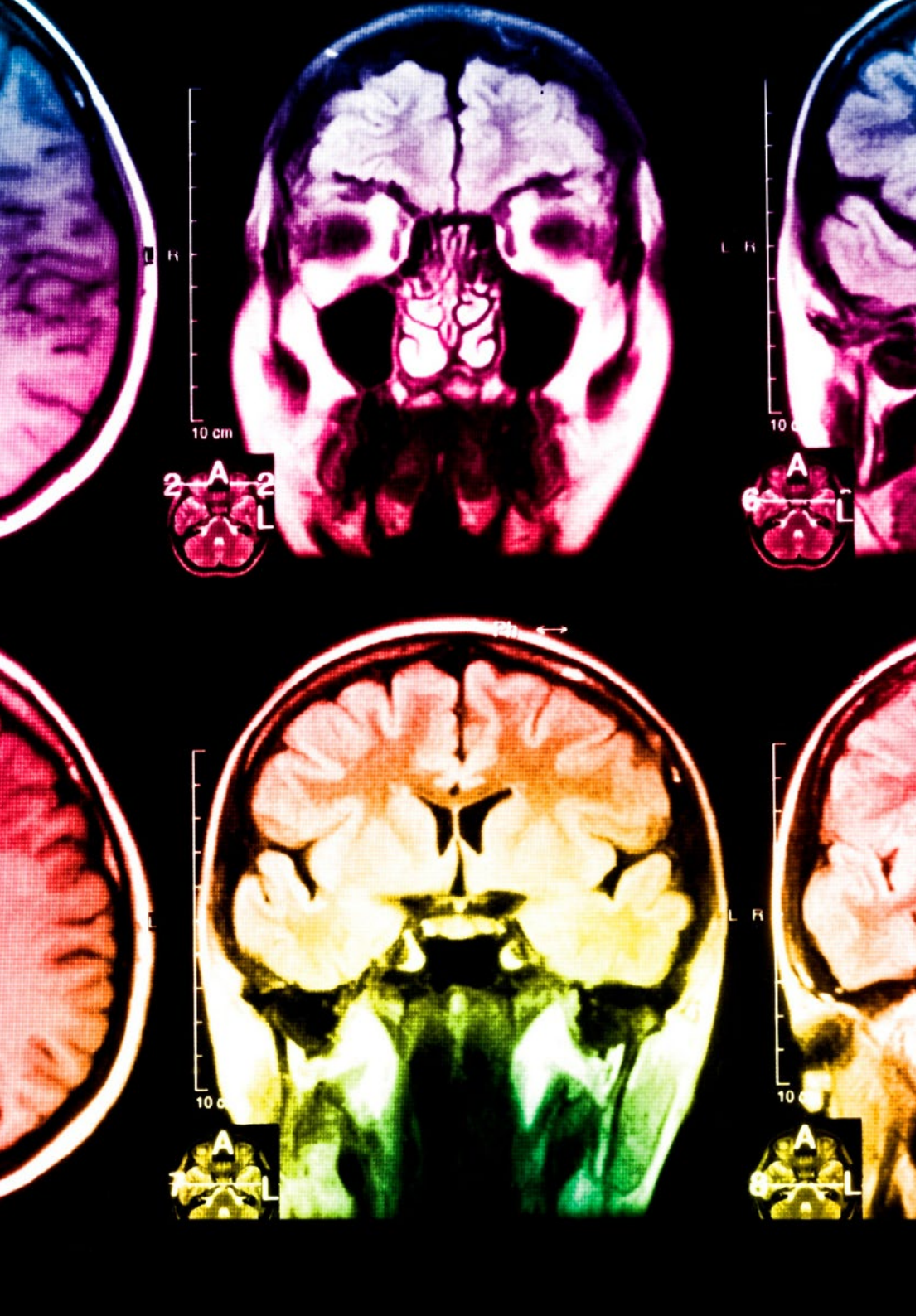
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

Im Jahr 2019 erzielten wir die besten Lernergebnisse aller spanischsprachigen Online-Universitäten der Welt.

Bei TECH lernen Sie mit einer hochmodernen Methodik, die darauf ausgerichtet ist, die Führungskräfte der Zukunft zu spezialisieren. Diese Methode, die an der Spitze der weltweiten Pädagogik steht, wird Relearning genannt.

Unsere Universität ist die einzige in der spanischsprachigen Welt, die für die Anwendung dieser erfolgreichen Methode zugelassen ist. Im Jahr 2019 ist es uns gelungen, die Gesamtzufriedenheit unserer Studenten (Qualität der Lehre, Qualität der Materialien, Kursstruktur, Ziele...) in Bezug auf die Indikatoren der besten spanischsprachigen Online-Universität zu verbessern.



In unserem Programm ist das Lernen kein linearer Prozess, sondern erfolgt in einer Spirale (lernen, verlernen, vergessen und neu lernen). Daher wird jedes dieser Elemente konzentrisch kombiniert. Mit dieser Methode wurden mehr als 650.000 Hochschulabsolventen mit beispiellosem Erfolg in so unterschiedlichen Bereichen wie Biochemie, Genetik, Chirurgie, internationales Recht, Managementfähigkeiten, Sportwissenschaft, Philosophie, Recht, Ingenieurwesen, Journalismus, Geschichte, Finanzmärkte und -instrumente fortgebildet. Dies alles in einem sehr anspruchsvollen Umfeld mit einer Studentenschaft mit hohem sozioökonomischem Profil und einem Durchschnittsalter von 43,5 Jahren.

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.

Nach den neuesten wissenschaftlichen Erkenntnissen der Neurowissenschaften wissen wir nicht nur, wie wir Informationen, Ideen, Bilder und Erinnerungen organisieren, sondern auch, dass der Ort und der Kontext, in dem wir etwas gelernt haben, von grundlegender Bedeutung dafür sind, dass wir uns daran erinnern und es im Hippocampus speichern können, um es in unserem Langzeitgedächtnis zu behalten.

Auf diese Weise sind die verschiedenen Elemente unseres Programms im Rahmen des so genannten Neurocognitive Context-Dependent E-Learning mit dem Kontext verbunden, in dem der Teilnehmer seine berufliche Praxis entwickelt.

Dieses Programm bietet die besten Lehrmaterialien, die sorgfältig für Fachleute aufbereitet sind:

Studienmaterial

Alle didaktischen Inhalte werden von den Fachleuten, 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 das audiovisuelle Format angewendet, um die Online-Arbeitsmethode von TECH zu schaffen. All dies mit den neuesten Techniken, die in jedem einzelnen der Materialien, die dem Studenten zur Verfügung gestellt werden, qualitativ hochwertige Elemente bieten.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

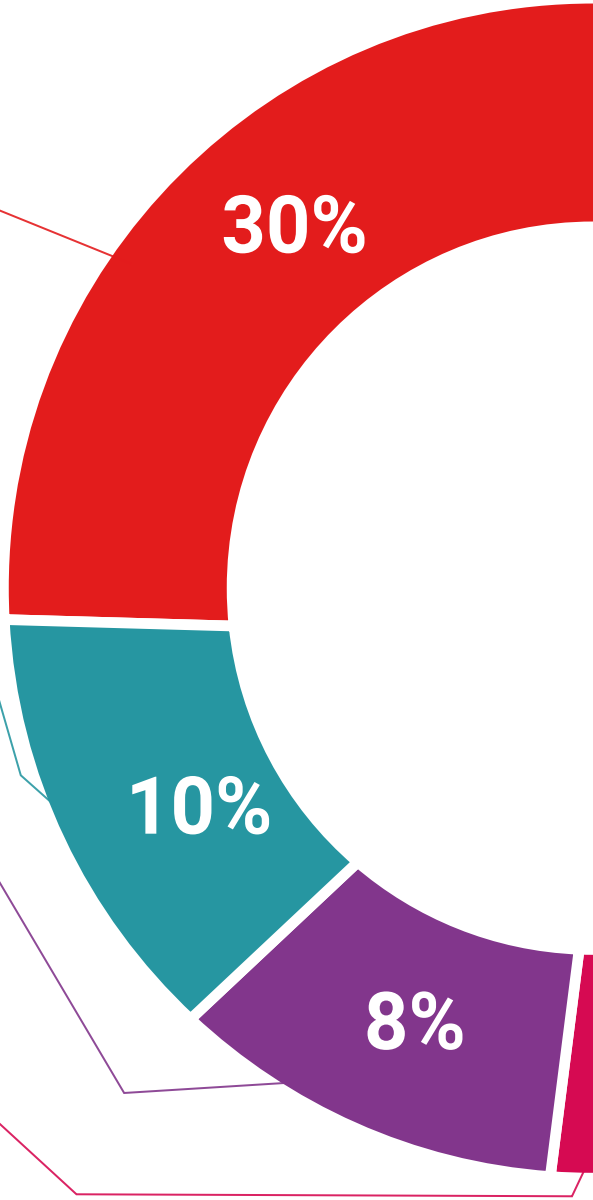
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

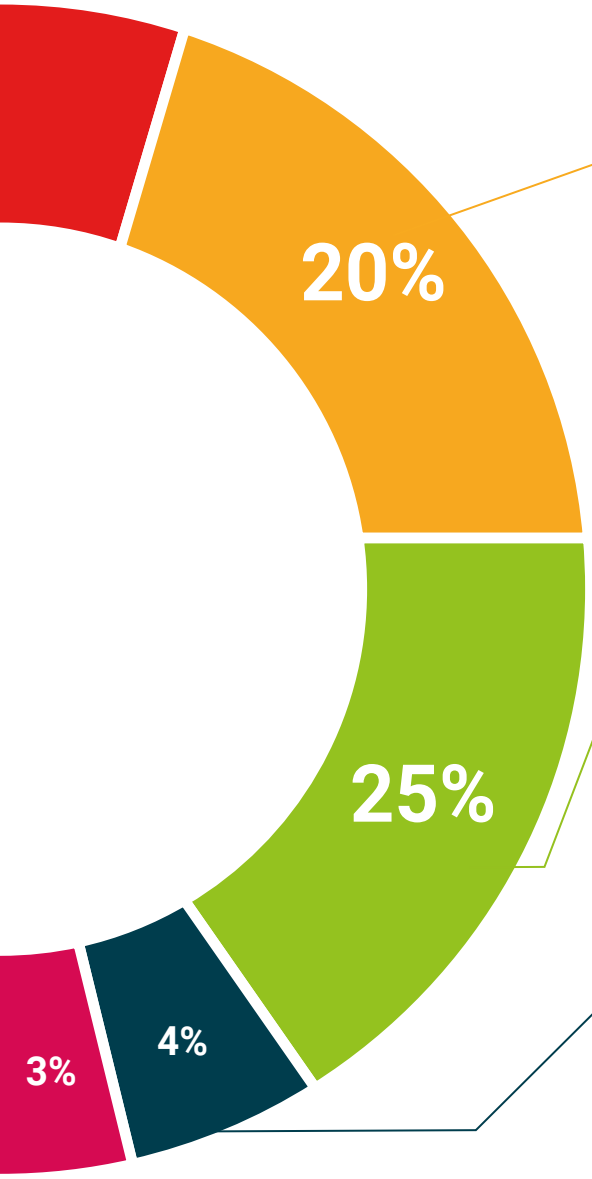
Übungen für Fertigkeiten und Kompetenzen

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.

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente und internationale Leitfäden, u. a. In der virtuellen Bibliothek von TECH hat der Student Zugang zu allem, was er für seine Fortbildung benötigt.





Case Studies

Sie werden eine Auswahl der besten Fallstudien vervollständigen, die speziell für diese Qualifizierung ausgewählt wurden. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.

Interaktive Zusammenfassungen

Das TECH-Team präsentiert die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, die Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu vertiefen.

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

Testing & Retesting

Die Kenntnisse des Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass der Student überprüfen kann, wie er seine Ziele erreicht.

07

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)**

Anzahl der offiziellen Arbeitsstunden: **3.000 Std.**


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	Stunden	Kategorie
1º	Cyberintelligenz und Cybersicherheit	100	OB
1º	Host-Sicherheit	100	OB
1º	Netzwerksicherheit (Perimeter)	100	OB
1º	Smartphone-Sicherheit	100	OB
1º	IoT-Sicherheit	100	OB
1º	Ethisches Hacking	100	OB
1º	Reverse Engineering	100	OB
1º	Sichere Entwicklung	100	OB
1º	Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware	100	OB
1º	Forensische Analyse	100	OB
1º	Sicherheit in Design und Entwicklung von Systemen	100	OB
1º	Architekturen und Modelle für die Informationssicherheit		
1º	Informationssicherheits-Managementsystem (ISMS)	100	OB
	IT-Sicherheitsmanagement		
1º	Richtlinien für das Management von Sicherheitsvorfällen	100	OB
1º	Risikoanalyse und IT-Sicherheitsumgebung	100	OB
1º	Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen	100	OB

Kurs	Modul	Stunden	Kategorie
2º	Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen	100	OB
2º	Kryptographie in der IT	100	OB
2º	Identitäts- und Zugriffsmanagement in der IT-Sicherheit	100	OB
2º	Sicherheit bei Kommunikation und Softwarebetrieb	100	OB
2º	Sicherheit in Cloud-Umgebungen	100	OB
2º	Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme	100	OB
2º	Sicherheit der Kommunikation von IoT-Geräten	100	OB
2º	Business Continuity Plan in Verbindung mit Sicherheit	100	OB
2º	Praktische Sicherheitspolitiken für die Notfallwiederherstellung	125	OB
2º	Implementierung von physischen und ökologischen	125	OB
2º	Sicherheitspolitiken im Unternehmen	125	OB
2º	Richtlinien für sichere Kommunikation im Unternehmen	125	OB
2º	Organisatorische Aspekte der Informationssicherheitspolitik	125	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: **24 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **o nline**

Weiterbildender Masterstudiengang

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

tech technologische universität