Titel der Präsentation: "Grundlagen der IT-Sicherheit"
I. Einführung
A. Kurze Vorstellung von Prof. Dr. Norbert Pohlmann
B. Überblick über das Institut für Internet-Sicherheit (if(is))
II. Einordnung der Vorlesung "Grundlagen der IT-Sicherheit"
A. Zielgruppe und notwendige Voraussetzungen
1. Bachelor-Studiengang Informatik
a) Pflichtmodul in der Studienrichtung Praktische Informatik
b) Wahlpflichtmodul in der Studienrichtung Technische Informatik
2. Wahlpflichtmodul für Bachelor-Studiengänge Medieninformatik und Wirtschaftsinformatik
B. Stundenumfang und Struktur
1. 4 SWS, unterteilt in Vorlesungen, Übungen und Praktikum
III. Lernziele der Vorlesung
A. Verständnis von möglichen Angriffen und Gegenmaßnahmen
B. Kenntnisse über die Funktionsweise von Sicherheitskomponenten und -systemen
C. Erfahrungen in der Ausarbeitung und Präsentation neuer Themen aus dem IT-Sicherheitsbereich
D. Praktische Erfahrungen mit Sicherheitssystemen
E. Wichtigkeit der IT-Sicherheit
IV. Inhalte der Vorlesung
A. Einführung in die IT-Sicherheitslage und -strategien
B. Wissen zur Cyber-Sicherheit: Motivationen, Kategorien und Angriffsvektoren
C. Kryptographie und technologische Grundlagen für Schutzmaßnahmen
D. Verfahren und Prinzipien der Authentifikation
E. Veränderungen und Herausforderungen in der Internet-Sicherheit
V. Praktikum und Übungen
A. Bedeutung und Organisation des Praktikums
B. Themen für Ausarbeitungen und Vorträge
VI. Unterlagen und Literatur
A. Folien und andere Unterlagen
B. Empfohlene Bücher und Zeitschriften
C. Online-Ressourcen zum Vertiefen des Wissens
VII. Abschluss und Diskussion
A. Fragen und Antworten
B. Feedback und weiterführende Ideen.
Schlüsselkonzepte zur Vertiefung:
1. Cyber-Sicherheit: Verständnis der grundlegenden Bedrohungen und Gegenmaßnahmen im Bereich der Informationstechnologie. Dieser Bereich umfasst Themen wie Sicherheitsstrategien, Angriffsvektoren und die aktuellen Herausforderungen im Bereich der Internet-Sicherheit.
2. Kryptographie: Auseinandersetzung mit den technologischen Grundlagen für Schutzmaßnahmen wie Private-Key-Verfahren, Public-Key-Verfahren und Hashfunktionen.
3. Authentifikationsverfahren: Vorstellung von grundlegenden Prinzipien, Algorithmen und Verfahren, die zur Verifizierung von Benutzern in IT-Systemen verwendet werden.
4. Praktische Übungen: Während der Vorlesung wird Wert auf praktische Erfahrungen gelegt, sei es durch Übungen, Vorträge oder ein Praktikum. Diese ermöglichen den Studierenden, das theoretische Wissen anzuwenden und konkret mit IT-Sicherheitslösungen zu arbeiten.
5. Wichtigkeit der IT-Sicherheit: Neben der rein technischen Komponente wird auch die gesellschaftliche Bedeutung von IT-Sicherheit betont. Ein tieferes Verständnis für die Auswirkungen von Cyberbedrohungen soll die Studenten dazu motivieren, sich intensiv mit diesem Thema auseinanderzusetzen.
Die Präsentation sollte mit ausreichenden Beispielen und gegebenenfalls Diagrammen oder Illustrationen angereichert werden, um komplexe Punkte zu verdeutlichen. Das Ziel ist es, den Studierenden eine klare und verständliche Einführung in die IT-Sicherheit zu geben.