



Einstieg in die Cybersicherheit: *Introduction to Cybersecurity* und *Cybersecurity Essentials*

21.4.2018

Prof. Dr. Heiko Knospe
TH Köln, Institut für Nachrichtentechnik
heiko.knospe@th-koeln.de

Technology
Arts Sciences
TH Köln

Agenda

- 1. Network Academy TH Köln**
- 2. Introduction to Cybersecurity**
- 3. Cybersecurity Essentials**
- 4. Vergleich der Kurse**
- 5. Integration in einen Hochschulkurs über IT-Sicherheit**
- 6. Ausblick**

Academy TH Köln

- Seit über 10 Jahren am Institut für Nachrichtentechnik, Fakultät für Informations-, Medien- und Elektrotechnik.
- Bachelor- und Masterstudiengänge in
 - Technische Informatik
 - Elektrotechnik
 - Communication Systems and Networks
- 5 Instruktoren (vier Professoren, ein Lehrbeauftragter)

Academy Kurse an der TH Köln

- CCNA R&S Exploration 1 - 4
- CCNA Security
- IoT Fundamentals
- Cybersecurity Essentials
- Introduction to Cybersecurity
- Linux Essentials, Programming Essentials in C, C++

Zu meiner Person

- Vorlesungen Mathematik, Kryptographie und IT-Sicherheit
- Aktiv in den Kursen CCNA Security, Introduction to Cybersecurity, Cybersecurity Essentials, IoT Fundamentals: Big Data and Analytics
- Cisco Certifications CCNA Routing & Switching und CCNA Security

Cybersecurity Kurse

- Introduction to Cybersecurity:
 - Beginning Level, 15 hours
 - Self paced or Instructor-led
 - keine Voraussetzungen
 - kein Instruktor Training erforderlich
 - Self-enroll page
- Cybersecurity Essentials:
 - Intermediate Level, 30 hours
 - Self paced or Instructor-led
 - Introduction to Cybersecurity Kurs empfohlen
 - Instruktor Training optional
 - Self-enroll page

Introduction to Cybersecurity

- 1. The Need for Cybersecurity:
 - Daten, Angriffe, Hacker - Angreifer, Cyberwarfare
- 2. Attacks, Concepts and Techniques
 - Arten von Schwachstellen, Malware, Infiltration und Angriffe
- 3. Protecting your Data and Privacy
 - Schutz der eigenen Geräte und Daten, Passwörter, 2-Faktor Authentifikation, Verschlüsselung, Backup etc.
- 4. Protecting the Organization
 - Kill Chain, Netzwerksicherheit, Firewall, IDS, IPS, Tools
- 5. Your Future in Cybersecurity



Quelle: Cisco

Beispiel: Introduction to Cybersecurity



Cyber Kill Chain



The Kill Chain in Cyberdefense

In cybersecurity, the Kill Chain is the stages of an information systems attack. Developed by Lockheed Martin as a security framework for incident detection and response, the Cyber Kill Chain is comprised of the following stages:

- Stage 1. Reconnaissance** - The attacker gathers information about the target.
- Stage 2. Weaponization** - The attacker creates an exploit and malicious payload to send to the target.
- Stage 3. Delivery** - The attacker sends the exploit and malicious payload to the target by email or other method.
- Stage 4. Exploitation** - The exploit is executed.
- Stage 5. Installation** - Malware and backdoors are installed on the target.
- Stage 6. Command and Control** - Remote control



Quelle: Cisco

Cybersecurity Essentials

- 1. A World of Experts and Criminals
 - Experten, Angreifer, Arten von Bedrohungen und Angriffen
- 2. The Cybersecurity Cube
 - CIA (Vertraulichkeit, Integrität, Verfügbarkeit)
 - Gegenmaßnahmen, auch organisatorischer Art
 - ISO 27000 Sicherheitsstandards, Fokus auf ISO 27001 und 27002, Abgrenzung ISMS und Maßnahmen nicht immer deutlich
- 3. Cybersecurity Threats, Vulnerabilities and Attacks
 - Verschiedene Typen von Malware und Angriffen gegen Netzwerke, Systeme und Applikationen

Cybersecurity Essentials

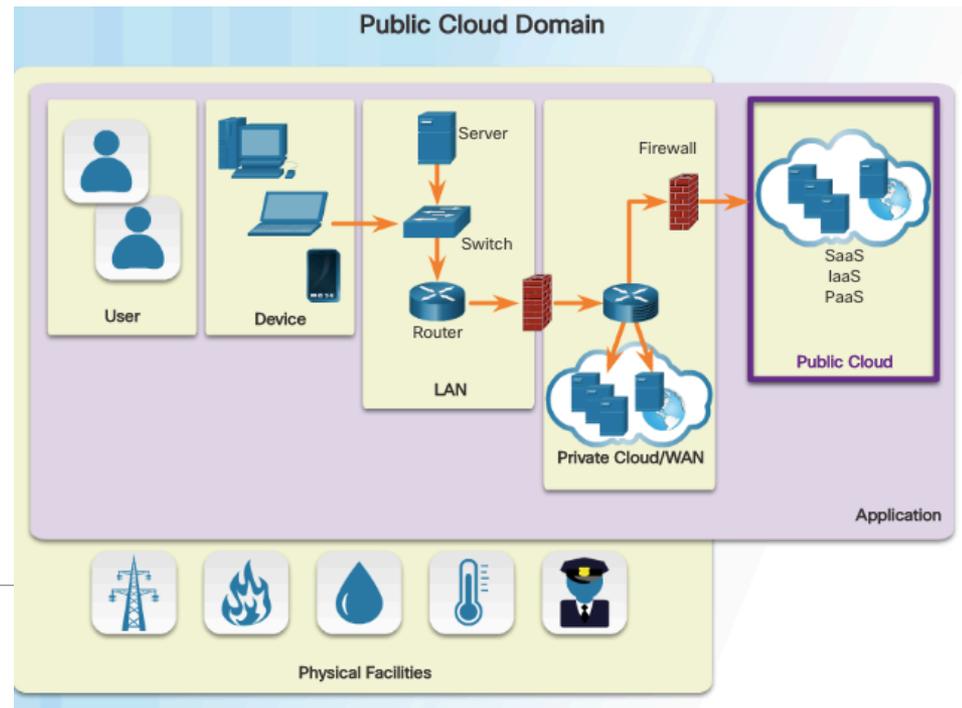
- 4. The Art of Protecting Secrets
 - Kryptographie (historisch, Vigenère, wenig relevant)
 - Symmetrische Verschlüsselung
 - Asymmetrische Verschlüsselung
 - Verschleierungstechniken, Steganographie
- 5. The Art of Ensuring Integrity
 - Hashverfahren, Message Authentication Codes
 - Digitale Signaturen
 - X.509 Zertifikate
 - Integrität in Datenbanken

Cybersecurity Essentials

- 6. The Five Nines Concept
 - Hochverfügbarkeit und Maßnahmen
 - Incident Response und Disaster Recovery
 - Verschleierungstechniken, Steganographie
- 7. Protecting a Cybersecurity Domain
 - Sicherheit von System und Mobilgeräten
 - Datensicherheit
 - Serversicherheit, Zugriffskontrolle, sichere Protokolle
 - Netzwerksicherheit: Switches, Router etc.
 - Physische Sicherheit. Zugang, Überwachung etc.

Cybersecurity Essentials

- 8. Becoming a Cybersecurity Expert
 - Cybersecurity Domains
User, Geräte, LAN, WAN, Private and Public Cloud, Software
 - Ethik, Richtlinien, Gesetze, (US-) Datenschutz
 - Security Jobs

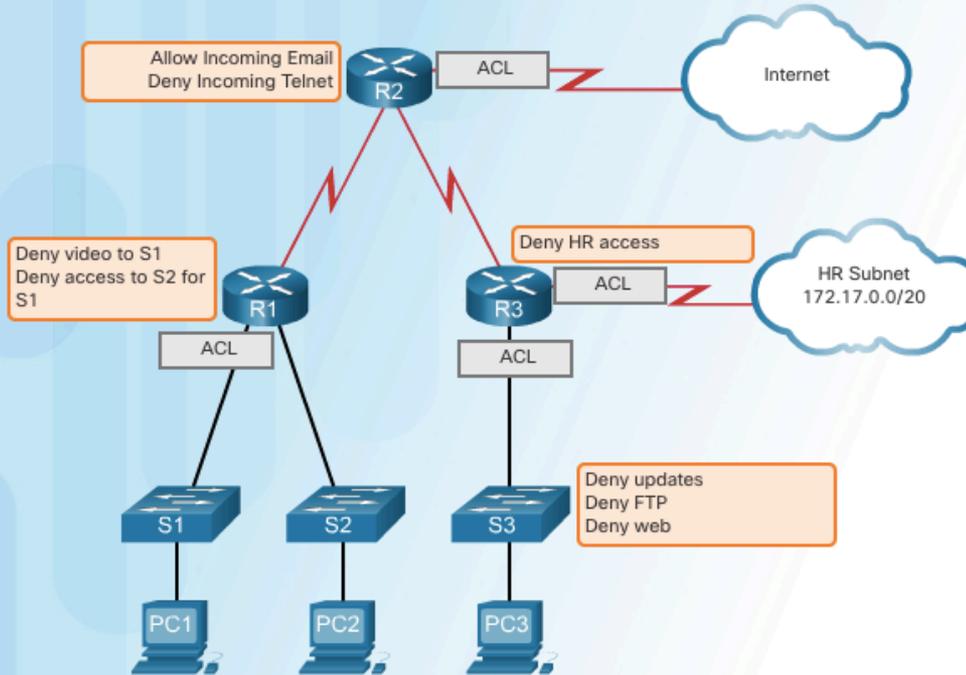


Quelle: Cisco

Beispiel: Cybersecurity Essentials



What Is an ACL?



Switches, Routers, and Network Appliances

Network devices ship with either no passwords or default passwords. Change the default passwords before connecting any device to the network. Document the changes to network devices and log the changes. Lastly, examine all configuration logs.

The following sections discuss several measures that an administrator can take to protect various network devices.

Switches

Network switches are the heart of the modern data communication network. The main threat to network switches are theft, hacking and remote access, attacks against network protocols like ARP/STP or attacks against performance and availability. Several countermeasures and controls can protect network switches including improved physical security, advanced configuration, and implementing proper system updates and patches



Vergleich

	Intro- duction	Essentials	IT Sec Kurs
Bewusstsein für Sicherheit	😊😊	😊😊	😊
Bedrohungen und Angriffe	😊	😊	😊😊
Sicherheits- maßnahmen	😐	😊	😊😊
Job Umfeld	😊	😊😊	😞
Theorie	😐	😐	😊

Vergleich: Hochschulkurse IT-Sicherheit

- Kryptographie
 - Mathematische Grundlagen (insbesondere Diskrete Strukturen, Zahlentheorie, Algebra)
 - Aktuelle Verfahren, z.B. SHA-3, ECC u.a.
 - Beweisbare Sicherheit
- Zugriffskontrolle und Sicherheitsmodelle
 - Authentifikation und Schlüsselvereinbarung, AKE Protokolle, Zugriffskontrollmodelle
- Netzwerksicherheit
 - LAN Sicherheit, IPsec, TLS (vgl. CCNA Security), Websicherheit
- Sicherheitsmanagement, Sicherheitsstandards, Gesetze
 - ISMS, ISO 27001 und ISO 27002, IT-Grundschutz, Risikomanag.
 - Datenschutz, DSGVO
 - Sicherheitsbewertung: Common Criteria

Integration in Hochschulkurse IT-Sicherheit

- Introduction to Cybersecurity Kurs zur Einführung und Motivation für das Thema Sicherheit (auch vor der ersten Vorlesung)
 - Online-Exam (Aufgabe und Lösungen leider im Internet)
- Cybersecurity Essentials nach einigen Vorlesungswochen, parallel zu Verfahren der Authentifikation und Zugriffskontrolle
 - Praktikum mit Cisco Ubuntu Linux VM: Benutzeraccounts und ACLs, Netzwerk-Scan, Password Cracking
 - Online Exam
- Cybersecurity Kurse geben praxisbezogene und betriebliche Sicht, z.B. Kapitel Protecting a Cybersecurity Domain
 - Themen der IT Integration fehlen häufig in Hochschulkursen
 - Kryptographie, Theorie, Details zu Protokollen und ihre Implementierung sowie Sicherheitsmanagement fehlen dagegen weitgehend in Cybersecurity Kursen

Fazit und Ausblick

- Cybersecurity Kurse (insbesondere der Essentials Kurs) sind sinnvolle Ergänzung zu einer Vorlesung über IT-Sicherheit
 - Praxisorientierung, insbesondere für Sys-Admins
 - Expertenniveau schwerer zu erreichen: tiefere Betriebssystem-, Netzwerk- und Softwarekenntnisse erforderlich
 - Positives Feedback von Studierenden, gute Online Plattform, beschränkter Aufwand, beliebte Zertifikate
- Als alleinige Grundlage von Hochschulkursen aber nicht geeignet (Niveau und fachliche Tiefe)
- Alternativer CCNA Security Kurs nur für einen Teil der Studierenden geeignet (CCNA Routing & Switching erforderlich)
- Neuer Cyber Ops Kurs interessante Ergänzung zu IT-Sicherheit
 - Sicherheit von Betriebssystemen und Netzwerken wird eingehender behandelt (ohne CCNA R&S vorauszusetzen)