

NETWORK SECURITY DIBY MANIYAL

CHRISTIAN BERG

WER BIN ICH UND WAS MACH ICH HIER



SEIT 1989 IN DER IT

SEIT 1998 BEI SCHWEICKERT

**DIPLOM-BETRIEBSWIRT DER
DATENVERARBEITUNG (BA)**

AB 2002 SECURITY

**INFORMATIONSSICHERHEITS-
BEAUFTRAGTER**

DHBW – CYBER SECURITY

LAUT LEHRPLAN



**Informatik
Cyber Security**

STUDIENGANGSMODULE INFORMATIK

MATHEMATIK	Lineare Algebra Analysis	Angewandte Mathematik Statistik	
INFORMATIK	Theoretische Informatik I & II Technische Informatik I	Theoretische Informatik III Technische Informatik II	
PROGRAMMIEREN	C Programmierung Einführung in JAVA		
SOFTWARE ENGINEERING		Software Engineering I	Software Engineering II
DATENBANKEN		Grundlagen der Datenbanken	
KOMMUNIKATIONS- UND NETZTECHNIK		Netztechnik Labor Netztechnik Signale und Systeme I	
IT-SICHERHEIT			IT-Sicherheit
STUDIENARBEIT			Studienarbeit

STUDIENRICHTUNGSMODULE CYBER SECURITY

KERNMODULE	Cyber Security Basics Einführung in die Kryptologie		Network Security Security by Design
WAHLMODULE	Web Engineering I & II Labor Mobile App-programmierung	Ausgewählte Themen des IT-Rechts IT-Sicherheitsmanagement Social Engineering	Data Security Labor Data Security Kryptoanalyse Digitale Forensik Labor Digitale Forensik Angriffsmethoden Penetration Testing

THEMEN

LAUT LEHRPLAN

LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN

Sichere Unternehmensnetze

PRÄSENZZEIT

36

SELBSTSTUDIUM

39

Perimeterschutz, z.B. Firewall, IDS, IPS, Sandboxing
Security Information and Event Management (SIEM) Systeme
Mail- und andere Gateways
SIEM Technology im Netzwerk
Verwaltung von Zertifizierungsstellen
NAC, Authentifizierungstechnologien
Malware, Viren, Trojaner, Spyware
Hochverfügbarkeit, Clustering, Hardening
Distributed Denial of Service (DDoS) Angriffe
Next Generation Firewalls
Anwendung von Kryptographie auf Netzwerke, Fallstricke
IoT Security

Labor Netzwerksicherheit


24

51

Praktische Anwendung sicherer Unternehmensnetzwerke



DHBW – NETWORK SECURITY

- Von Oktober bis Ende Dezember 2022
 - Fachbereich „Cyber Security“ – 5. Semester
 - 36 Schulstunden Vorlesung, 24 Schulstunden Labor
 - 09-13h, aber kann kürzer oder länger sein (tbd)
- 
- A solid red horizontal bar with a diagonal cut on the left side, located at the bottom right of the slide.

VORSTELLUNGSRUNDE

„WAS NÜTZT ES GUT ZU SEIN, WENN KEINER ES WEISS?“

- Name
- Firma
- Generelle Tätigkeit beim Unternehmen
- Aktuelles bzw. letztes Thema/Projekt



SEMESTER - ABLAUF

Oktober

Vorstellung
Ablauf

Grundlagen

Grundlagen

Security
Gateways

Encryption

Security
Gateways

November

Malware
Ransomware

Nextgen
Firewall

Scanning/
OSINT

Scanning/
OSINT

IOT Security

Normen/
Hardening

Dezember

Cloud Security

SIEM

SIEM

NAC

Klausur

THEORIE

PRAXIS

SEMESTER ÜBERSICHT

LERNEINHEITEN

GRUNDLAGEN

- LAN
- WLAN
- WAN

SECURITY GATEWAYS

- Firewall
- IDS/IPS
- WEB/WAF

ENCRYPTION

- VPN
- PKI
- SSL-Terminierung

MALWARE

- Malware
- Ransomware Bericht
- Ransomware Prevention

SCANNING

- OSINT
- Vulnerabilities
- Scanning

IOT SECURITY

- Grundlagen
- IOT-Hacking

- Supply-Chain-Angriffe

NORMEN

- Normen
- Organisatorische Sicherheit
- Hardening

CLOUD SECURITY

- DNS/MAIL
- Application Gateways
- as a Service

SIEM

- Grundlagen
- MITRE-Framework
- Incidents

NAC

- Grundlagen
- Authentication
- Interaktion

ABLAUF AM BEISPIEL „GRUNDLAGEN“

LERNEINHEITEN, THEORIE

3 BLÖCKE Á 45MIN, 5-10MIN PAUSE DAZWISCHEN

Grundlagen

LAN

WLAN

WAN



ABLAUF 45MIN SLOT

Intro

Historie

Stand der Technik

Absicherung

Tools, Links, Tips

ANGRIFFSVEKTOREN

HAUSAUFGABE



Eine Folie

- Gängige Angriffsvarianten
- Evtl. spektakulärer Hack
- Aufwand vs. Nutzen

Linkliste

Hausaufgab

ANGRIFFSVEKTOREN

HAUSAUFGABE



Eine Folie/Seite

- z.B. Gängige Angriffsvarianten
- Evtl. spektakulärer Hack

LAN

WLAN

WAN (Router)

Homework



CYBER SECURITY WETTER

HAUSAUFGABE



Was geschah letzte Woche?


- Evtl. spektakulärer Hack
- Schwerwiegende Sicherheitslücken?
- ALLE



LABORE

LABOR-DAY, ALLE 2 WOCHEN, MOODLE/BBB

Themen

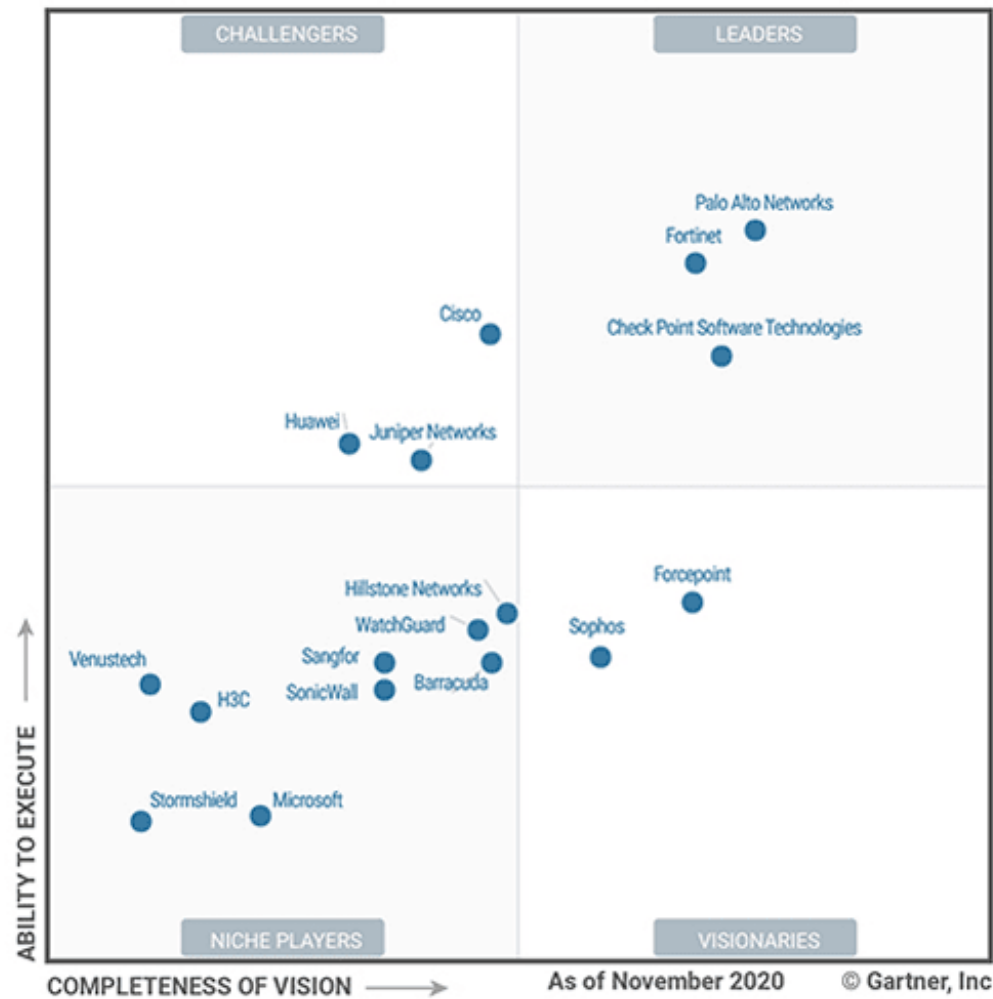
- Sniffing (mit Notebook und Wireshark)
 - Firewalling
 - Next-Generation-Firewalling
 - Scanning/OSINT
 - Boss of the SOC
 - Offenes Thema/Abschluss (z.B. NAC)
- 

ABORE



HERSTELLER

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

Juniper

Barracuda

Huawei

Watchguard

Sonicwall

PFSense

FAST DOZENTEN



BKÜRZUNGEN

Quiz-Time II

LAN

WLAN

WAN

OSI

RFC

PKI

EDR

IPS

IEEE

TLS

SSL

SIEM

WAF

IETF

SDWAN

VPN

OSINT

ISO


IOT

NAC

Stand der Technik

DSGVO: unter Berücksichtigung des **Standes der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und ...

KRITIS: ... "angemessene Vorkehrungen zur Vermeidung von Störungen [...] ihrer informationstechnischen Systeme, Komponenten und Prozesse" nach dem "**Stand der Technik**" zu treffen und dies gegenüber dem BSI nachzuweisen.



DEFINITION NACH BUNDESVERFASSUNGSGERICHT 1978

niedrig

↑

Allgemeine
Anerkennung

↓

hoch



niedrig

↑

Bewährung in der
Praxis

↓

hoch

BUNDESVERBAND IT-SICHERHEIT E.V. (TELETRUST)

Bundesverband IT-Sicherheit e.V.



IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

technischer und organisatorischer Maßnahmen

2020

3	Technische und organisatorische Maßnahmen (TOM)	15
3.1	Allgemeine Hinweise	15
3.2	Technische Maßnahmen	18
3.2.1	Bewertung der Passwortstärke	18
3.2.2	Durchsetzung starker Passwörter	20
3.2.3	Multifaktor-Authentifizierung	21
3.2.4	Kryptographische Verfahren	24
3.2.5	Verschlüsselung von Festplatten	25
3.2.6	Verschlüsselung von Dateien und Ordnern	27
3.2.7	Verschlüsselung von E-Mails	28
3.2.8	Sicherung des elektronischen Datenverkehrs mit PKI	30
3.2.9	Einsatz von VPN (Layer 3)	33
3.2.10	Verschlüsselung auf Layer 2	35
3.2.11	Cloudbasierter Datenaustausch	37
3.2.12	Datenablage in der Cloud	38
3.2.13	Nutzung von mobilen Sprach- und Datendiensten	40
3.2.14	Kommunikation mittels Instant-Messenger	41
3.2.15	Management mobiler Geräte	43
3.2.16	Routersicherheit	44
3.2.17	Netzwerküberwachung mittels Intrusion Detection System	46
3.2.18	Schutz des Web-Datenverkehrs	48
3.2.19	Schutz von Webanwendungen	49
3.2.20	Fernzugriff auf Netzwerke / Fernwartung	51
3.2.21	Server-Härtung	53
3.2.22	Endpoint Detection & Response Plattform	56
3.2.23	Internetnutzung mit Web-Isolation	58
3.2.24	Angriffserkennung und Auswertung (SIEM)	60
3.3	Organisatorische Maßnahmen	62
3.3.1	Standards und Normen	62
3.3.2	Prozesse	65
3.3.2.1	Sicherheitsorganisation	66
3.3.2.2	Anforderungsmanagement	67
3.3.2.3	Management des Geltungsbereichs	69
3.3.2.4	Management der Informationssicherheits-Leitlinie	69
3.3.2.5	Risikomanagement	69
3.3.2.6	Management der Erklärung zur Anwendbarkeit	69
3.3.2.7	Ressourcenmanagement	70
3.3.2.8	Wissens- und Kompetenzmanagement	70
3.3.2.9	Dokumentations- und Kommunikationsmanagement	70
3.3.2.10	IT-Servicemanagement	70
3.3.2.11	Management der Erfolgskontrolle	72
3.3.2.12	Verbesserungsmanagement (kontinuierlicher Verbesserungsprozess)	73
3.3.3	Sichere Softwareentwicklung	74
3.3.4	Audits und Zertifizierung	77
3.3.5	Schwachstellen- und Patchmanagement	72

INSTUFUNG NACH HANDREICHUNG DER TELETRUST

Quiz-Time

Starke Passwörter

Einsatz von VPNs

Schutz des Web-Datenverkehrs
(ausgehend)

Multifaktor-Authentifizierung



Netzwerk-überwachung mit
IPS

Verschlüsselung
von Festplatten

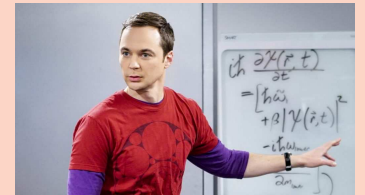
Management
mobiler Geräte

Verschlüsselung
von E-Mails

Server-Härtung

Schutz von
Webanwendungen
(eingehend)

Wissenschaft & Forschung



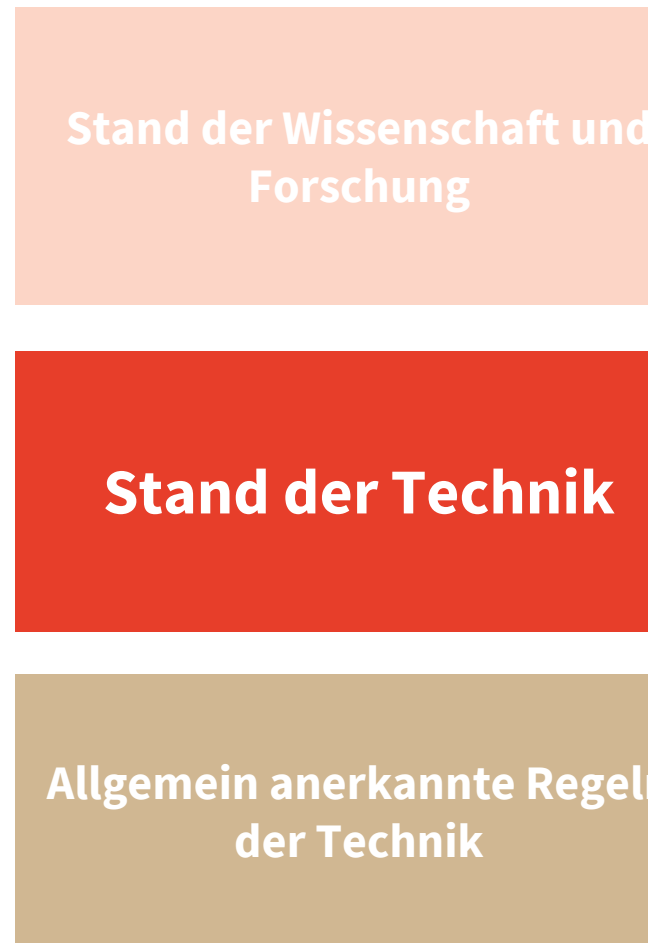
Stand der Technik

Allgemein anerkannte Regel



INSTUFUNG NACH HANDREICHUNG DER TELETRUST

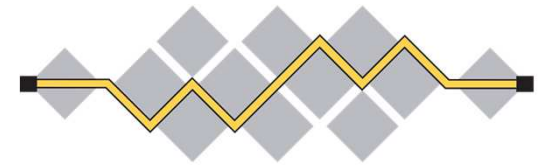
ösung



VERBÄNDE



802.3
802.11



I E T F®



RFC



TCP/UDP



NORMUNG



OSI-Modell



ISO27001



HAUSAUFGABE ALLE

Rot markierte (falls nicht bekannt) nachlesen

LAN

WLAN

WAN

OSI

RFC

PKI

EDR

IPS

IEEE

VPN

SSL

SIEM

WAF

IETF

SDWAN

VPN

OSINT

ISO

IoT

NAC

ISO/OSI Modell

PLANUNG

25-27. Oktober 2022



01-03.11 §8A Prüfung



ANGRIFFSVEKTOREN

HAUSAUFGABE



Eine Folie

- z.B. Gängige Angriffsvarianten
- Evtl. spektakulärer Hack

LAN

WLAN

WAN (Router)

Homework – bis nächstes Mal



FRAGEN?