

ISF HS 2019

Victor Fernández

Dezember 2019

Inhaltsverzeichnis

I	Einführung (SW 01)	3
1	Einführung	3
II	Kryptographie (SW 02-04)	3
2	Symmetrische Kryptographie	4
3	Asymmetrische Kryptographie	4
4	Zertifikate und SSL-TLS	5
III	Angriffe (SW 05-06)	5
5	Angriffe auf Webanwendungen	5
6	Angriffe auf Protokollebene	6
IV	Management (SW 07-09)	6
7	Standards & Frameworks, ISMS	6
8	Risiko-Management und IT-Grundschutz	6
9	Awareness	7
V	Access Control (SW 10)	7
10	Access Control	7
VI	Multi-Party-Computation (SW 11)	8
11	Cryptographic Protocols	8
12	Secret Sharing	8
13	Zero Knowledge Proof	8
VII	Quantum (SW 12)	8
14	Quantum Computing and Quantum Cryptography	9

VIII	WAF, Federations (SW 13)	9
15	Firewalls	9
16	Federations	9
IX	Talks (SW 14)	9
17	Malware	9
18	WAF	9

Teil I

Einführung (SW 01)

1 Einführung

Einführung in das Thema „Management von Informationssicherheit“

Daten, Information und Wissen Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.

Missbrauch Informationen müssen vor Missbrauch geschützt werden

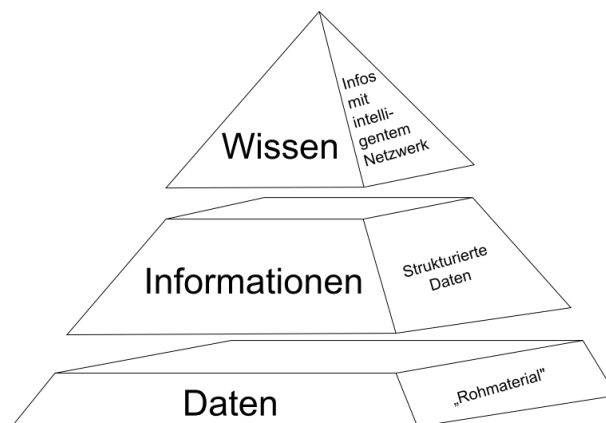


Abbildung 1: Wissenspyramide

Motivation / Bedrohungen

Was gefährdet die Informationen? Welche Gefährdungen/Bedrohungen gibt es?

- Nicht vorsätzliche (zufällige) Gefährdungen/Bedrohungen
 - Naturgewalten (Blitz, Hagel, Unwetter, Erdbeben, Hochwasser, etc.)
 - Ausfall von Strom oder Telekommunikation
 - Technische Pannen, z.B. Fehler von Hard- und/oder Software
 - Bedienerfehler / Fahrlässigkeit der Mitarbeitenden
- Vorsätzliche Gefährdungen/Bedrohungen
 - Böseartiger Code (Viren, Würmer, Trojaner, etc.)
 - Informationsdiebstahl
 - Angriffe (von Skript-Kiddies bis Hacker)
 - Wirtschaftsspionage („was die Konkurrenz wissen möchte“)
 - Missbrauch der IT-Infrastruktur

Grundbegriffe

Zutritts-, Zugangs-, Zugriffskontrolle

- **Zutrittskontrolle:** Schutz des physischen Systems (Bsp. Serverraum)
- **Zugangskontrolle:** Schutz des logischen Systems (Bsp. Betriebssystem)
- **Zugriffskontrolle:** Daten-bezogen; Schutz der Operationen (Bsp. Dateisystem)

Teil II

Kryptographie (SW 02-04)

2 Symmetrische Kryptographie

Sie verstehen was Steganographie ist

TODO

Sie verstehen was Private-Key-Kryptographie ist, welche Arten von Sicherheit es gibt und welche Angriffsarten auf Verschlüsselung existieren

TODO

Sie können „klassische“ symmetrische Verschlüsselungsverfahren wie Ceasar cipher, Vigenère cipher, one-time pad anwenden und verstehen die Vor- und Nachteile bzw. Schwachstellen dieser Verfahren

TODO

Sie wissen welche modernen Verschlüsselungsalgorithmen in der Praxis verwendet werden und was deren Eigenschaften sind

TODO

Sie verstehen was eine Hashfunktion ist und welche Eigenschaften eine kryptographische Hashfunktion ausmachen, bzw. was es heisst, wenn eine Hashfunktion gebrochen ist

TODO

Sie kennen moderne Hashfunktionen und wissen welche Eigenschaften diese haben

TODO

Sie kennen Anwendungen von Hashfunktionen

TODO

Sie wissen was ein keyed Hash (HMAC) ist und wofür dieser verwendet werden kann

TODO

Sie kennen die „Best-practices“ zu Passwortsicherheit und wissen, gegen welche Angriffe diese schützen

TODO

3 Asymmetrische Kryptographie

Sie verstehen was Public-Key-Kryptographie ist, worauf deren Sicherheit basiert und wie sie zur Verschlüsselung, für Signaturen und zur Authentisierung verwendet werden kann

TODO

Sie kennen die gängigen asymmetrischen Verschlüsselungs- und Signaturalgorithmen und wissen, worauf deren Sicherheit basiert

TODO

Sie wissen wie Diffie-Hellmann-Schlüsselaustausch bzw. ElGamal-Verschlüsselung funktioniert

TODO

Sie wissen was kryptographisch sichere Zufallszahlen sind und wo diese verwendet werden

TODO

Sie wissen was eine elektronische Signatur ausmacht

TODO

Sie wissen wie hybride Verschlüsselung bzw hybride Signaturen funktionieren

TODO

4 Zertifikate und SSL-TLS

Sie kennen die verschiedenen Arten von „Trust“

TODO

Sie wissen was eine Public-Key-Infrastruktur, eine Certificate Authority und ein Zertifikat ist, wofür und wie diese verwendet werden und wie Zertifikate ausgestellt und revoziert werden

TODO

Sie wissen was SSL/TLS ist, welche Funktionalität es erreicht und wie das Protokoll konzeptionelle abläuft

TODO

Teil III

Angriffe (SW 05-06)

5 Angriffe auf Webanwendungen

TODO

Sie wissen was eine Webanwendung ausmacht, wie HTTP funktioniert

TODO

Sie wissen was eine Session ist und welche Eigenschaften einer Session bei welchen Angriffen wichtig sind bzw wie sie gegen gewisse Angriffe Schutz bieten

TODO

Sie kennen sicherheitsrelevante Header

TODO

Sie verstehen wie ein Cross-Site-Request-Forgery-Angriff abläuft und wie man sich dagegen schützen kann

TODO

6 Angriffe auf Protokollebene

Sie kennen die Grundbegriffe der Anwendungssicherheit

TODO

Sie kennen Beispiele von Angriffen auf verschiedenen Ebenen des Protokollstacks und wissen was diese bewirken

TODO

Sie verstehen wie ein Cross-Site-Scripting/SQL-injection/Social-Engineering-Angriff abläuft und wie man sich dagegen schützen kann

TODO

Teil IV

Management (SW 07-09)

7 Standards & Frameworks, ISMS

Sie wissen, was ein ISMS ist und wie man damit umgeht

TODO

Sie kennen die wichtigsten Standards der Informationssicherheit

TODO

Sie finden sich in den Standards ISO 27001 und 27002 zurecht

TODO

Sie verstehen die Grundzüge der BSI-Standards (BSI=Bundesamt für Sicherheit in der Informationstechnik, Deutschland)

TODO

Sie kennen die Struktur und Grundziele des NIST CyberSecurityFrameworks

TODO

8 Risiko-Management und IT-Grundschutz

Das Risikoanalyse-Verfahren verstehen

TODO

Die Unterschiede zum Grundschutzverfahren kennen

TODO

Eine einfache Risikoanalyse durchführen können

TODO

Sie verstehen die Idee, die Ziele und die Konzepte des IT-Grundschutz-Vorgehens

TODO

Sie kennen den Aufbau der IT-Grundschutz-Kataloge und deren Anwendungsweise

TODO

Sie können die Teilschritte zum Aufbau eines Sicherheitskonzeptes nach IT-Grundschutz durchführen, kombinierte Risikoanalyse

TODO

9 Awareness

Sie verstehen die Wichtigkeit der «Awareness »

TODO

Sie kennen verschiedene Prozesse und Vorgehensweisen für die Initiierung, Durchführung und Erfolgsprüfung einer Awareness-Kampagne und können diese anwenden

TODO

Sie kennen die relevanten Erfolgsfaktoren der Mitarbeiter-Sensibilisierung und -Schulung und können diese in einer Kampagne umsetzen

TODO

Teil V

Access Control (SW 10)

10 Access Control

Sie kennen verschiedene Arten der Authentisierung, wissen wie diese technisch ablaufen und was deren Vor- und Nachteile sind

TODO

Sie wissen wie verschiedene Authentisierungstoken technisch funktionieren, was deren Vor- und Nachteile sind und wie sie beim Login oder bei der Transaktionsbestätigung im e-Banking eingesetzt werden

TODO

Sie wissen was Authentisierung, Autorisierung ist, warum diese wichtig sind und wie Angriffe darauf ablaufen

TODO

Teil VI

Multi-Party-Computation (SW 11)

Sie kennen einfache Beispiele von verteilten sicheren Berechnungen und verstehen wie die entsprechenden Protokolle ablaufen

TODO

Sie kennen Arten von Sicherheit von verteilten sicheren Berechnungen und wie diese angegriffen werden können

TODO

Sie wissen welche Eigenschaften elektronisches Geld ausmachen und kennen die technischen Grundlagen von Bitcoin

TODO

11 Cryptographic Protocols

12 Secret Sharing

13 Zero Knowledge Proof

Sie wissen was Zero-Knowledge-Proofs sind und wie diese ablaufen

TODO

Teil VII

Quantum (SW 12)

Sie wissen was ein Quantencomputer ist und was ihn von einem „klassischen“ Computer unterscheidet

TODO

Sie verstehen welchen Einfluss die Existenz eines Quantencomputers auf die Kryptographie hat

TODO

Sie verstehen wie Quantenschlüsselaustausch funktioniert

TODO

14 Quantum Computing and Quantum Cryptography

Teil VIII

WAF, Federations (SW 13)

15 Firewalls

Sie wissen was die Aufgaben einer Firewall sind

TODO

Sie verstehen die Funktionsweise einer WAF und wie sie eine Webanwendung vor Angriffen schützen kann

TODO

16 Federations

Sie verstehen wie Authentisierung mit Identity Federation abläuft, was die Voraussetzungen dafür sind und was die Vor- und Nachteile von Federations sind

TODO

Teil IX

Talks (SW 14)

17 Malware

Sie verstehen, welche Arten von Malware es gibt, welche Massnahmen gegen Malware sinnvoll sind und wie diese wirken

TODO

18 WAF

Sie verstehen wo Machine-Learning in einer WAF eingesetzt werden kann und was eine Machine-Learning-Ansatz vom „herkömmlichen“ Einsatz einer WAF unterscheidet

TODO

Sie kennen Beispiele von Angriffen, welche mittels Machine-Learning auf einer WAF erkannt werden konnten

TODO