IT-Sicherheit

Organisatorisches und Grundbegriffe

Version vom 25.09.2024

Organisatorisches

- Vorlesungstermine: Mittwoch, 08:45
- Sprechstunde: nach Vereinbarung via https://calendly.com/uhrmann
- Fragen: jederzeit in der Vorlesung
  im Moodle-Forum
  oder via johann.uhrmann@haw-landshut.de

- Prüfung: schriftlich, 90 Minuten, keine Hilfsmittel

  Nur für BA-IF Studierende mit Studienstart vor WS2019/20 und BA-WIF mit Studienstart vor WS2021/22: 60 Minuten Prüfung

Moodle

Zu dieser Vorlesung

- Kursname: 2024/25 WiSe IT-Sicherheit (Uhrmann)
- Key: InfoSec2025
- Inhalte:
  - Skript, Übungen, Übungsblätter
  - Feedback-Foren
  - Vorbereitungsmaterial
  - Aufgaben
  - Praktikumsaufgaben und -termine

Spontane Gedanken zu IT-Sicherheit

1. Welche drei Begriffe fallen Ihnen spontan zum Thema IT-Sicherheit ein?
2. Gehen Sie auf folgende URL: https://partici.fi , Code **4533 7069** und tragen dort die Begriffe ein.

Ziele und Inhalte der Vorlesung

- Ziele von Informationssicherheit (wann ist ein System sicher)
- Bedrohungen, Verwundbarkeiten
- Kryptographie
- Netzwerksicherheit
- sichere Softwareentwicklung
- sicherer IT-Betrieb

am realen Beispiel

IT-Zoom
[https://www.it-zoo dsoftware-18750/]

Angriff auf die IT

Hacker fordern Lösegeld von der Caritas

13. September 2022, 17:16 Uhr | Lesezeit: 2 min

Der Betrieb in der Caritas-Zentrale und in den Einrichtungen läuft nach dem Hacker-Angriff im "analogen Modus" weiter. (Foto: privat)

Oberbayerns größter Wohlfahrtsverband ist Opfer einer Cyber-Attacke geworden: Kriminelle haben eine Schadsoftware eingeschleust und Daten verschlüsselt.

Von Joachim Mölter

Süddeutsche Zeitung, 13.09.2022

(Hacker-) Ethik: Beispiel 1

Bamberg/Landshut – **Er führte einen der größten deutschsprachigen Drogen-Verkaufsplätze im Darknet – jetzt bekam der Landshuter Student Louis K. (23) dafür die Quittung vor Gericht. Das Urteil: vier Jahre und neun Monate Haft!**

Das Landgericht Bamberg sprach den ehemaligen Studenten unter anderem wegen Betreibens krimineller Handelsplattformen im Internet und des bandenmäßigen Drogenhandels schuldig. Die Richter ordneten auch die Unterbringung in einer Entziehungsanstalt an.

Für die Richter war klar: Louis K. hielt die Plattform „Deutschland im Deep Web 3" im Darknet, einem verborgenen Teil des Internets, zwischen Oktober 2021 und März 2022 am Laufen.

[Thomas Gautier, bild.de, 17.12.2023]

(Hacker-) Ethik: Beispiel 2 – Responsible Disclosure

3.4 RESEARCHER

Siemens thanks the following parties for their efforts:

- Luca Simbürger, Luca Hofschuster, Lukas Kahnert, Jakob Lachermeier, Christian Costa, Simon Huber, Lukas Sas Brunschier, Florian Freiberger, Florian Burger, Marie-Louise Oostveen, Magdalena Thomeczek, and Johann Uhrmann from Landshut University of Applied Sciences.
- Max Hirschberger, Simon Hofmann, and Peter Knauer from Augsburg University of Applied Sciences.

[ICS Advisory: Siemens SICAM MMU, SICAM T, and SICAM SGU https://www.cisa.gov/news-events/ics-advisories/icsa-20-196-03]

Ziele

Vertraulichkeit

- Zugriff auf Informationen ist auf autorisierte Personen begrenzt. Nicht autorisierte Personen können auf die Informationen nicht zugreifen.

Integrität

- Informationen dürfen nur von Personen verändert werden, die dazu autorisiert sind. Strengere Auslegung: Die Informationen müssen korrekt, konsistent und vor Manipulation geschützt sein.

Verfügbarkeit

- Autorisierte Personen und Systeme können auf die Informationen und Ressourcen zugreifen, wenn diese benötigt werden.

Wird eines dieser Ziele verletzt, dann gilt das System nicht länger als sicher!

Weitere, optionale Ziele der Informationssicherheit

- Auditierbarkeit

  Sicherheitsrelevante Eigenschaften, Prozesse und Mechanismen können eingesehen und überprüft werden.
- Non-Repudiation

  Nutzer können Aktionen am System nicht abstreiten. Ihre Aktionen werden mit ihren Identitäten verknüpft.
- Accountability

  Das System stellt sicher, dass (sicherheitsrelevante) Änderungen am System immer einer Person / Nutzer zugeordnet werden können.
- Privacy

  Personenbezogene Daten werden nach den geltenden Vorschriften geschützt.
- Authentizität

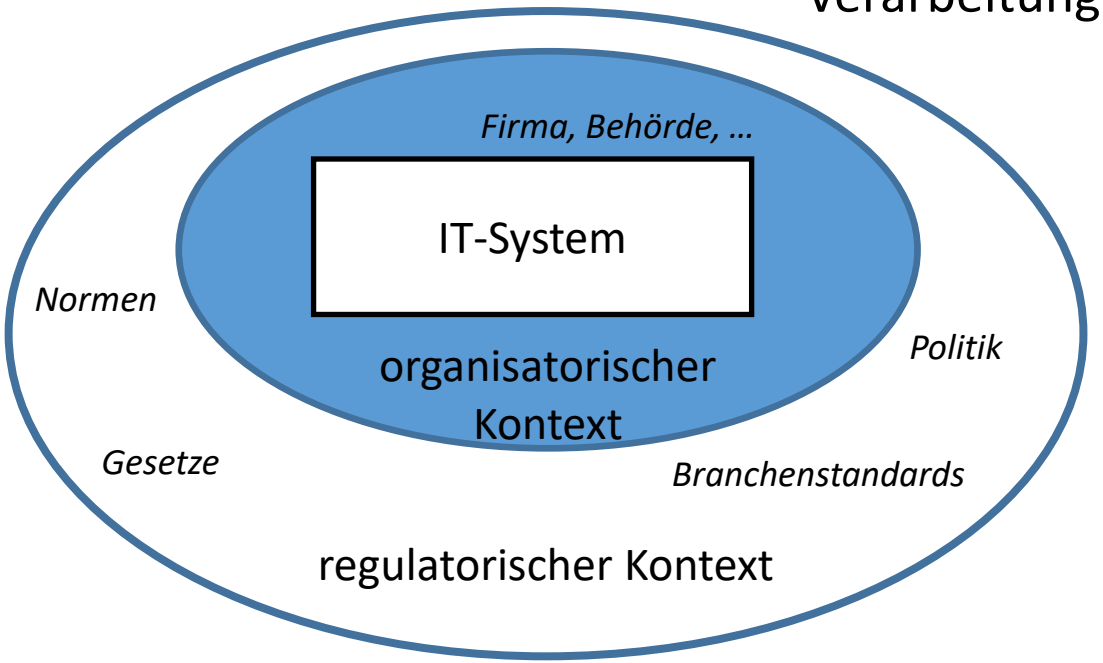
  Informationen können nachprüfbar einem bestimmten Sender zugeordnet werden.
- Deniability

  Inhalte einer Kommunikations-beziehung oder die Beteiligung können im Nachhinein nicht nachgewiesen werden.

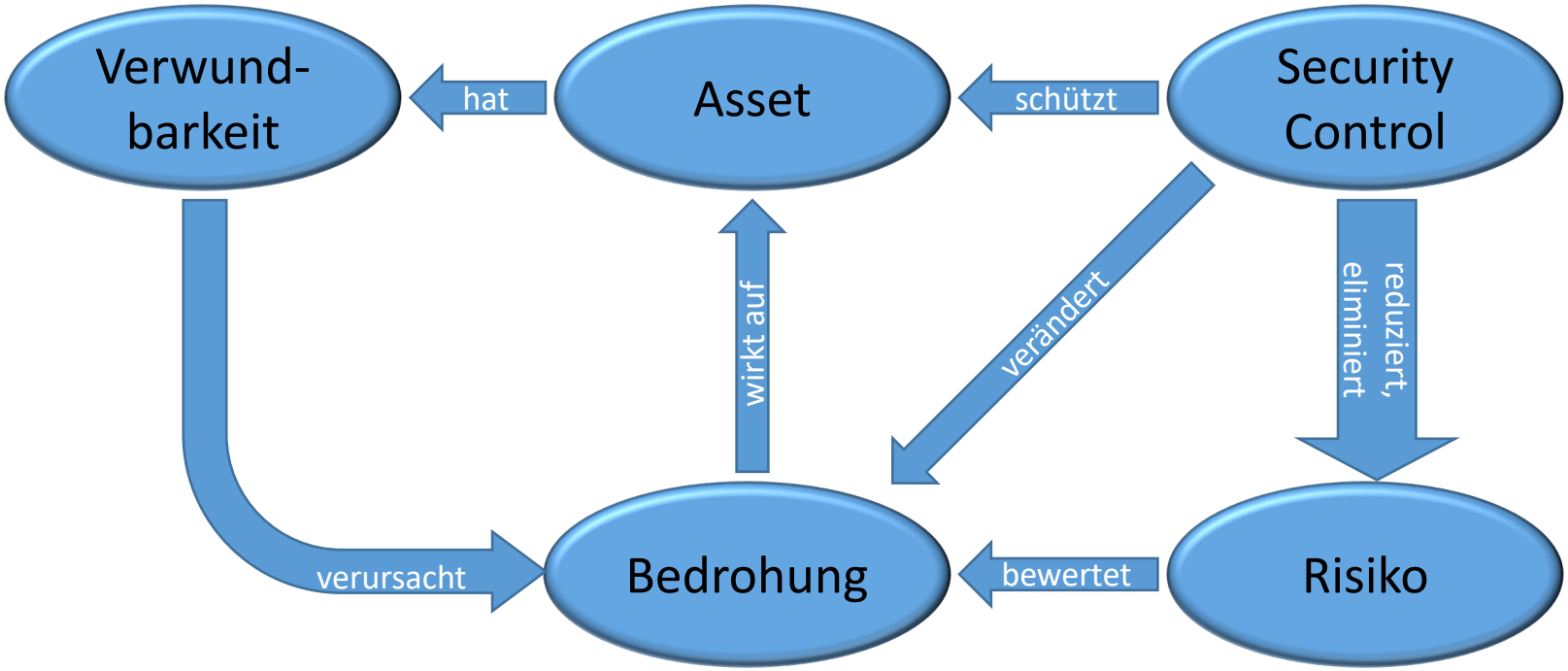
Grundbegriffe: IT-System

Ein IT-System ist ein offenes oder geschlossenes, dynamisches, technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen.

[C. Eckert, IT-Sicherheit]



Grundbegriffe



Asset

- ist Ressource, Prozess, Produkt oder System.
- besitzt einen Wert für die Organisation.
- muss geschützt werden.

- kann System, Netzwerk, Rechner, physikalische Einrichtung sein.
- kann virtuell sein.
- kann Information und Wissen aber auch z.B. das Ansehen einer Marke sein.

Bedrohung

- Umstand oder Ereignis, das auf ein Asset
  - einen unerwünschten Effekt haben kann.
  - schädlich wirken kann.
- Bedrohungen können Ursachen in der Umwelt (Überschwemmung, Feuer) haben oder von Menschen verursacht werden (menschliche Fehler oder Vorsatz).

Verwundbarkeit

- Fehlen oder Schwäche im Schutz eines Assets.

➔Verursacht, dass eine Bedrohung
  ➔überhaupt auftritt
  ➔mit höherer Wahrscheinlichkeit oder Häufigkeit auftritt
  ➔einen höheren Schaden verursacht

- Verwundbarkeiten in Software werden von MITRE und den angeschlossenen Softwareherstellern / CERTs mit CVEs (common vulnerabilities and exposures) versehen.

Beispiel: Heartbleed

CVE-ID

CVE-2014-0160 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- URL:http://www.securityfocus.com/archive/1/archive/1/534161/100/0/threaded
- EXPLOIT-DB:32745
- URL:http://www.exploit-db.com/exploits/32745
- EXPLOIT-DB:32764
- URL:http://www.exploit-db /32764
- 20140408 CVE-2014-0160

[http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160]

Bewertung von Schwachstellen mit CVSS

CVE-2020-10037 Detail

Current Description

A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information.

+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD **NIST:** NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

[National Institute for Standard and Technologies]

Risiko

- kennzeichnet die Kombination aus
  - der Wahrscheinlichkeit, dass eine bestimmte Quelle einer Bedrohung auf ein Informationssystem einwirkt (durch versehentliche oder absichtliche Auslösung) und
  - den Auswirkungen, die diese Bedrohung hat, falls sie tatsächlich eintritt
- wird umgangssprachlich häufig als Synonym zu „Bedrohung“ verwendet.
- Risikobewertungen können quantitiv oder qualitativ erfolgen.

Angriff

Ein Angriff ist ein nicht autorisierter Zugriff bzw. nicht autorisierter Zugriffsversuch auf ein System.

Es wird unterschieden nach aktiven und passivem Angriff:

- Bei passiven Angriffen wird unautorisiert aus Daten oder Netzwerkverbindungen gelesen. (Sniffing)
- Beispiele für aktive Angriffe sind Verändern, Entfernen, Unterdrücken, Fälschen, Zerstören von Informationen auf Netzwerkverbindungen oder Datenträgern.
- Aktive Angriffe können auch darauf abzielen, die Verfügbarkeit von Diensten oder Komponenten zu beeinträchtigen. (denial of service attack)

Security Control

Verschiedene Typen von Security Controls:

- Deterrent Control
  Verringert die Eintrittswahrscheinlichkeit eines Risikos
- Preventative Control
  Eliminiert das Risiko durch Entfernen der Schwachstelle
- Detective Control
  Erkennt eine Bedrohung und führt zur Auslösung eines…
- Corrective Control
  Verringert die Auswirkungen (Schadenshöhe) eines Risikos
- Compensating Control
  Ein Security Control, das an Stelle eines anderen verwendet wird, da es leichter umzusetzen ist. (z.B. bei organisatorische vs. technischen Controls)