IT-Sicherheit

Organisatorisches und Grundbegriffe

Version vom 10.10.2019

Organisatorisches

- Vorlesungstermine: Donnerstag, 08:45 – 10:15
- Sprechstunde: Dienstag, 09:00 nach Vereinbarung
- Fragen: jederzeit in der Vorlesung
  im Moodle-Forum
  oder via johann.uhrmann@haw-landshut.de
- Prüfung: schriftlich, 60 Minuten, keine Hilfsmittel

Moodle

Zu dieser Vorlesung

- Kursname:
  WS 18/19 IT-Sicherheit
  (Uhrmann)
- Key: INFOSEC19
- Inhalte:
  - Skript, Übungen, Übungsblätter
  - Feedback-Foren
  - Vorbereitungsmaterial
  - Aufgaben

Zur Professur Informationssicherheit

- Kursname:
  Prof. Dr. Uhrmann
- Key: uhrmann
- Inhalte:
  - Allgemeine Informationen zur Professur
  - Themen für Studienprojekte und Abschlussarbeiten

Spontane Gedanken zu IT-Sicherheit

1. Welche drei Begriffe fallen Ihnen spontan zum Thema IT-Sicherheit ein? (NICHT laut aussprechen)
2. Gehen Sie auf folgende URL: https://menti.com, Code **26 43 70** 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

Motivation

Bundeswahlleiter und BSI sind alarmiert
PC-Wahl habe nicht nur die Zielserver für die Übermittlung der Ergebnisse am Wahlabend voreingestellt. Auch das Passwort, das benötigt wird, um sich auf dem Server der nächsten Ebene einzuloggen, liefere es gleich mit. Damit niemand Unbefugtes an diese Passwörter kommt, sind sie in PC-Wahl verschlüsselt gespeichert. "Ein normaler Mensch kann die nicht auslesen, denn ich habe einen eigenen Kompressionsalgorithmus gebaut, da braucht es schon viel Gehirnschmalz, um den zu knacken", sagt PC-Wahl-Entwickler Berninger. Dem CCC gelang dies mühelos. Berninger hatte nicht damit gerechnet, dass die Hacker eine Vollversion seines Programms finden würden.

[zeit online, 07.09.2017,
http://www.zeit.de/digital/datenschutz/2017-09/bundestagswahl-wahlsoftware-hackerangriff-sicherheit-bsi-bundeswahlleiter/seite-3]

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

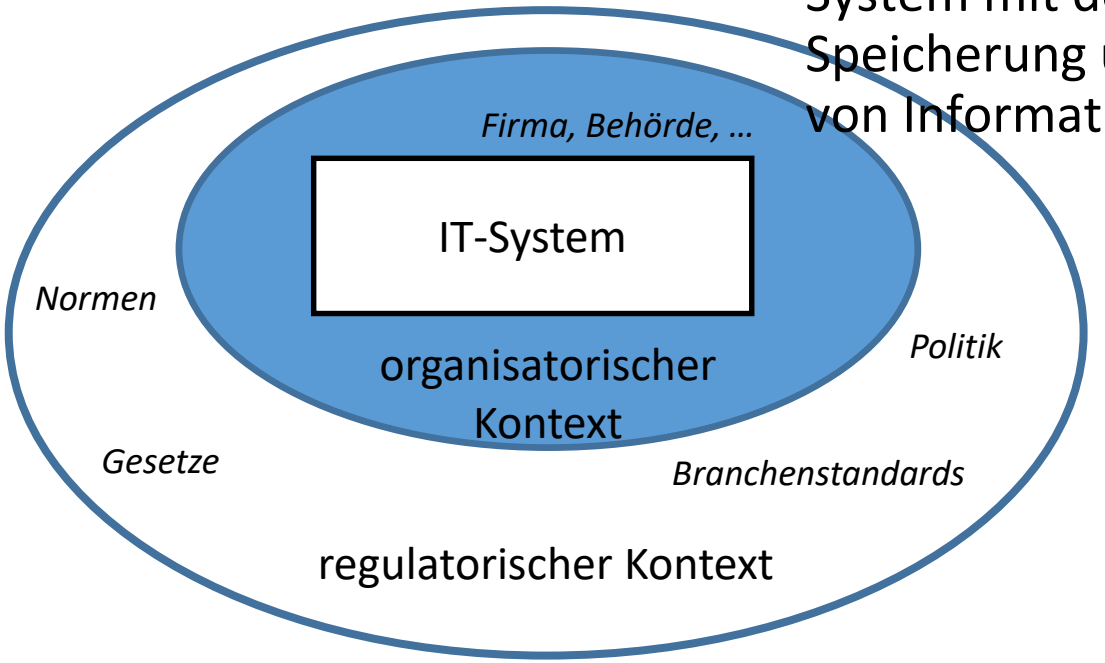
  Informationen können nachprüfbar einem bestimmten Sender zugeordnet werden.
- Deniability

  Inhalte einer Kommunikations-beziehung oder die Beteiligung können im Nachhinein nicht nachgewiesen werden. (Genau Gegenteil von Non Repudiation manchmal wichtig)

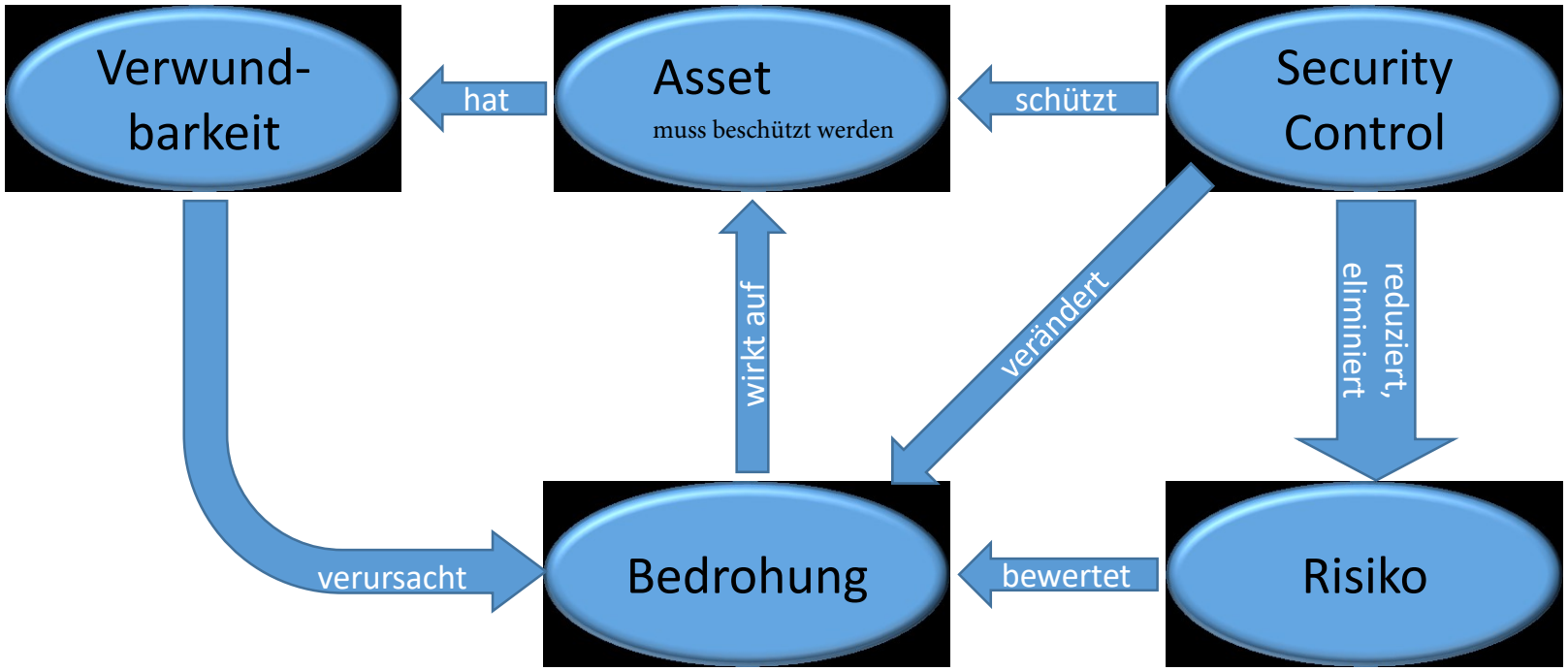
Grundbegriffe: IT-System

Ein IT-System ist ein offene oder geschlossenes(ein Hersteller, begrenzete Leute, zb AKW), 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

National Cyber Awareness System

Vulnerability Summary for CVE-2014-0160

Original release date: 04/07/2014

Last revised: 10/22/2015

Source: US-CERT/NIST

Overview

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.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information

"'Catastrophic' is the right word. On the scale of 1 to 10, this is an 11.
Half a million sites are vulnerable, including my own."

[Bruce Schneier]

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(genaue Zahlen (oft unmgl gerade im IT Bereich) oder qualitativ (gering,mittel,hoch reicht)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 - verringern des Imapct und Probability

Verschiedene Typen von Security Controls:

- Deterrent Control
  Verringert die Eintrittswahrscheinlichkeit eines Risikos
- Preventative Control
  Eliminiert das Risiko durch Entfernen der Schwachstelle, senkt die Eintrittswahrscheinlicheit auf null. Durch Patch. optimal
- Detective Control
  Erkennt eine Bedrohung und führt zur Auslösung eines Logs
- Corrective Control - zb Backup
  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)