Computersystemsicherheit

Prof. Marc Fischlin

Wintersemester 2018-2019

Inhaltsverzeichnis

1 Einleitung

1.1 Unsicherheit ist Überall

Komplexität ist der (erste) Feind der Sicherheit. Je komplexer Systeme sind, desto mehr potenzielle Schwachstellen haben sie. Der Trend ist zu immer komplexeren System, von Mikrowellen, die per App steuerbar sind, zu Autos, die ein WLAN besitzen oder eventuell sogar direkt über das Mobilfunknetz an das Internet angebunden sind.

Dass eine solche Entwicklung auch potenzielle Sicherheitsrisiken birgt, zeigt unter anderen eine relativ aktuelle Schwachstelle, die es Angreifern ermöglicht, Zugriff auf ein Auto zu erlangen, und gewisse Funktionen über WLAN zu steuern.

1.2 Lessons Learned

Sicherheit ist komplex. Es besteht aus vielen Komponenten, und ist meistens nur so gut wie das schwächste Glied. In dieser Veranstaltung geht es darum, die Sicherheit von Computersystemen zu verstehen.

1.3 Rechtliches

Diese Veranstaltung beinhaltet auch Informationen über Angriffsmöglichkeiten, die wichtig sind, um die Sicherheit von Computersystemen besser zu verstehen. Diese Möglichkeiten dürfen außerhalb des in der Veranstaltung vorgesehenen Rahmens (gegen Dritte) nicht verwendet werden, denn dies kann Rechtliche Konsequenzen haben, siehe Abbildung 1.

1.4 Worum geht es?

Bei der Computersystemsicherheit geht es um mehrere Aspekte. Dazu gehören Privacy, Datensicherheit (Access Control), Sicherheit von Netzwerken, Sicherheit und Anwender (Usability), Sicherheit auf Computern (Software, Hardware), Server-Sicherheit (Webserver).

Es gibt einen ISO-Standard zur Computersystemsicherheit, den ISO/IEC 27002 (2700X ist eine Serie von Standards zum Thema IT-Sicherheit). Dieser definiert eine Reihe von Bereichen, in denen Maßnahmen zur IT-Sicherheit getroffen werden müssen. In dieser Vorlesung werden folgende Bereiche behandelt:

- A.7: Human resource security
- A.9: Access control
- A.10: Cryptography
- A.12: Operations security

§ 202a Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten
Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten
(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

Abbildung 1: Gesetzeslage

- A.13: Communications security
- A.14: System acquisition, development and maintenance

1.5 Begriffe

Vulnerability Schwachstelle des Systems. Manche Vulnerabilities bekommen eine sogenannte CVE-Nummer[1].

Threat Bedrohung. Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann.

Threat Consequence Gefahr/Gefährdung. Folge, wenn Bedrohung auf Schwachstelle trifft.

Exploit Schadensvorfall. Konkreter Umstand oder Ereignis, durch das Schaden entsteht.

Countermeasure Gegenmaßnahme, um Schwachstelle oder Bedrohung zu mindern oder zu beseitigen.

[1] Siehe https://cve.mitre.org/ für mehr Informationen