

IT Sicherheit

Grundbegriffe & Motivation

Christoph Roschger

TGM Wien
Höhere Abteilung für Informationstechnologie

September, 2020

Security = ?

Security = ?

Security (lt. Oxford Dictionary)

The state of being free from danger or threat.

Security = ?

Security (lt. Oxford Dictionary)

The state of being free from danger or threat.

Safety = ?

Security = ?

Security (lt. Oxford Dictionary)

The state of being free from danger or threat.

Safety = ?

Safety (lt. Oxford Dictionary)

The condition of being protected from or unlikely to cause danger, risk, or injury.

- ▶ vgl. dt. "Sicherheit" in beiden Fällen



IT-Security = ?

Cyber-Security = ?

Information Security = ?

Digital Security = ?

Data Security = ?

Was soll geschützt werden?

Die CIA - Schutzziele

- ▶ Confidentiality
- ▶ Integrity
- ▶ Availability

Was soll geschützt werden?

Confidentiality

Vertraulichkeit

- ▶ Schutz von Informationen vor Bekanntgabe an Unbefugte
- ▶ Zugriff auf Informationen sollte nur auf Grund von einer **need-to-know** - Basis erfolgen
- ▶ Daten können nach Sensitivität und potentielltem Schaden kategorisiert werden.

Verwandte Prinzipien:

- ▶ Authentifizierung, Authorisierung, Verschlüsselung,...

Was soll geschützt werden?

Integrity

Integrität

- ▶ Schutz von Informationen davor, von Unauthorisierten verändert zu werden
- ▶ Korrektheit von Informationen
- ▶ Sicherstellung, dass Information beim Transport nicht manipuliert wird (Tampering)

Verwandte Prinzipien:

- ▶ Hashing, Digitale Signaturen, Non-repudiation, Tamper-evident packaging,...

Was soll geschützt werden?

Availability

Verfügbarkeit

- ▶ Sicherstellung, dass autorisierte Benutzer auch Zugriff auf Daten haben
- ▶ Sicherstellung, dass angebotene Dienste auch verfügbar sind

Verwandte Prinzipien:

- ▶ Fehlertoleranz, Redundanz, Backups, Testen,...

Was soll geschützt werden?

Die CIA-Schutzziele

Welche Sicherheitsziele betreffen die folgenden Bedrohungen?

- ▶ Netzwerk Sniffing
- ▶ DDoS-Attacke
- ▶ Rogue Wifi Access Point
- ▶ EMP
- ▶ Whistleblower
- ▶ Social Engineering
- ▶ Ransomware

Grundprinzipien

Minimalprinzip

Eine Anwendung sollte nur jene Operationen und Funktionen beinhalten, die für die Erfüllung der Anforderungen nötig sind. Alle weiteren Funktionen sollen entfernt bzw. deaktiviert werden.

- ▶ Welche Komponenten sind notwendig und welche Funktionen innerhalb der Komponenten?
- ▶ Prinzip KISS – Keep It Simple (and) Stupid
- ▶ Vgl. DSGVO – Minimalitätsgebot
- ▶ **Security Misconfiguration**: phpmyadmin, Debug Modes, phpinfo.php, .git-Verzeichnisse,...

Least Privilege Principle (J. Salzer)

“Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.”

- ▶ Arbeiten als Administrator
- ▶ Webserver als root laufen lassen
- ▶ ...

Grundprinzipien

Was soll im Fehlerfall passieren?

Fail-Open vs. Fail-Closed

Fail-Open Operation wird durchgeführt

Fail-Close Operation wird **nicht** durchgeführt

► Beispiel: Türschloss?

Grundprinzipien

Was soll im Fehlerfall passieren?

Fail-Open vs. Fail-Closed

Fail-Open Operation wird durchgeführt

Fail-Close Operation wird **nicht** durchgeführt

- ▶ Beispiel: Türschloss?
- ▶ Allgemein: Kommt auf die Anwendung an.

Grundprinzipien

No-Go: Security By Obscurity

Die Sicherheit eines Systems darf niemals von dessen Intransparenz abhängig sein.

Grundprinzipien

No-Go: Security By Obscurity

Die Sicherheit eines Systems darf niemals von dessen Intransparenz abhängig sein.

- ▶ vgl. das Kerckhoff'sche Prinzip in der Kryptographie:

Kerckhoff'sches Prinzip

Die Sicherheit eines Algorithmus darf nur von der Geheimhaltung des Schlüssels und nicht durch die Geheimhaltung des Algorithmus abhängig sein

- ▶ Bsp.: CSS Verschlüsselung bei DVDs

Vulnerability (lt. NIST)

“A **flaw or weakness** in system security procedures, design, implementation, or internal controls that could [...] result in a security breach or a violation of the system's security policy”

- ▶ veröffentlicht als **CVEs** (Common Vulnerabilities and Exposures): cve.mitre.org, www.cvedetails.com unter Mithilfe von **CNAs** (CVE Numbering Authorities)
- ▶ von MITRE www.mitre.org verwaltet
- ▶ **CVSS** (Common Vulnerability Scoring System) Score
- ▶ Typen: DoS, Code Execution, Overflow, Memory Corruption, Sql Injection, XSS, Directory Traversal, Http Response Splitting, Bypass something, Gain Information, Gain Privileges, CSRF, File Inclusion

Grundbegriffe

Ich habe ein Vulnerability gefunden - Was tun?

No Disclosure Kenntnis über Vulnerability wird nicht geteilt bzw. nicht veröffentlicht. Bsp: **Black hat hacker**, Verkauf, vertragl. Verpflichtungen,...

Grundbegriffe

Ich habe ein Vulnerability gefunden - Was tun?

No Disclosure Kenntnis über Vulnerability wird nicht geteilt bzw. nicht veröffentlicht. Bsp: **Black hat hacker**, Verkauf, vertragl. Verpflichtungen,...

Limited Disclosure Nur allgemeine Beschreibung ohne konkrete Details werden veröffentlicht

Grundbegriffe

Ich habe ein Vulnerability gefunden - Was tun?

No Disclosure Kenntnis über Vulnerability wird nicht geteilt bzw. nicht veröffentlicht. Bsp: **Black hat hacker**, Verkauf, vertragl. Verpflichtungen,...

Limited Disclosure Nur allgemeine Beschreibung ohne konkrete Details werden veröffentlicht

Full Disclosure Volle Veröffentlichung. Hersteller wird nicht bzw. nur sehr kurz vorher benachrichtigt Bsp.:
CVE-2019-16759

Grundbegriffe

Ich habe ein Vulnerability gefunden - Was tun?

No Disclosure Kenntnis über Vulnerability wird nicht geteilt bzw. nicht veröffentlicht. Bsp: **Black hat hacker**, Verkauf, vertragl. Verpflichtungen,...

Limited Disclosure Nur allgemeine Beschreibung ohne konkrete Details werden veröffentlicht

Full Disclosure Volle Veröffentlichung. Hersteller wird nicht bzw. nur sehr kurz vorher benachrichtigt Bsp.:
CVE-2019-16759

Responsible Disclosure Vorheriges Informieren des Herstellers mit Frist zur Veröffentlichung der Vulnerability (auch **Coordinated Disclosure**)

Grundbegriffe

Ich habe ein Vulnerability gefunden - Was tun?

No Disclosure Kenntnis über Vulnerability wird nicht geteilt bzw. nicht veröffentlicht. Bsp: **Black hat hacker**, Verkauf, vertragl. Verpflichtungen,...

Limited Disclosure Nur allgemeine Beschreibung ohne konkrete Details werden veröffentlicht

Full Disclosure Volle Veröffentlichung. Hersteller wird nicht bzw. nur sehr kurz vorher benachrichtigt Bsp.:
CVE-2019-16759

Responsible Disclosure Vorheriges Informieren des Herstellers mit Frist zur Veröffentlichung der Vulnerability (auch **Coordinated Disclosure**)

► vgl. Bug Bounty Programme

Grundbegriffe

Exploit (lt. Wikipedia)

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

Grundbegriffe

Exploit (lt. Wikipedia)

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

- ▶ Öffentliche exploits zB www.exploit-db.com gelistet.
- ▶ [Zero-day](http://zerodium.com) exploits: zerodium.com
- ▶ [Payload](#): Derjenige Teil eines Exploits, der die gewünschte Aktion ausführt
- ▶ [Metasploit](#): Software/Framework zum einfachen Anwenden von Exploits

Grundbegriffe

Hacking = ?

Grundbegriffe

Hacking = ?

Ursprünglich:

- ▶ kreative Funktionserweiterung oder Problemlösung auf ungewöhnliche Weise, um die Grenzen des Systems oder Gerätes zu erweitern
- ▶ vs. Cracking

Grundbegriffe

Hacking = ?

Ursprünglich:

- ▶ kreative Funktionserweiterung oder Problemlösung auf ungewöhnliche Weise, um die Grenzen des Systems oder Gerätes zu erweitern
- ▶ vs. Cracking

Heute:

- ▶ Umgehen von Sicherheitsmechanismen und Ausnutzen von Schwachstellen, um nicht autorisierten Zugang zu Computersystemen zu erhalten.
- ▶ black hat vs. white hat vs. grey hat

Exploit

Schadsoftware

Typen von Malware

Viren/Würmer Selbständige Verbreitung

Trojanisches Pferd Vorgabe anderer Funktionalitäten, zB.
KeePass, CCleaner

Spyware Ausspionieren des Benutzers

Adware Anzeige von Werbung

Rootkit Sehr gute Tarnung im System

Ransomware Erpressen des Benutzers

Cryptojacker Mining für Cryptowährungen

Botnet "Fernsteuerung" von vielen Computern gleichzeitig,
zB. für DDoS-Angriffe