rockenstein AG
Internet-Service-Provider

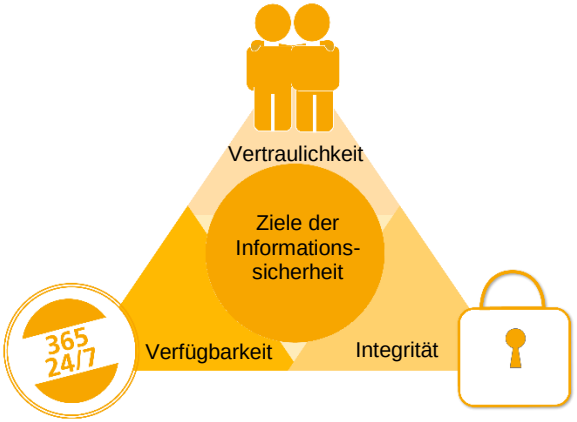
Datenübertragung und Sicherheit

Schutzziele der Informationssicherheit

Stand: 2021-10-26

Was ist Informationssicherheit?

„Als Informationssicherheit bezeichnet man Eigenschaften von technischen oder nicht-technischen Systemen zur Informationsverarbeitung,-speicherung und -lagerung, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen.“[1]



Informationssicherheit dient dem Schutz vor Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken. Durch die Fortschreitung der Digitalisierung und Automatisierung sind immer mehr Unternehmen von deren Informationstechnologie abhängig. Dazu zählen die Programme, die durch die IT gesteuert sowie die Informationen, die dadurch bereitgestellt werden. Die erhöhte Abhängigkeit birgt deshalb auch ein größeres Risiko für Angriffe jeglicher Art. Die Erstellung eines geeigneten Sicherheitskonzeptes sowie die Auswahl notwendiger Maßnahmen ist aufgrund dessen essenziell für jedes Unternehmen. Die Maßnahmen sollen sich an den drei wesentlichen Schutzzielen der Informationssicherheit Vertraulichkeit, Verfügbarkeit und Integrität orientieren, um die Gewährleistung gewisser Dateneigenschaften sicherzustellen.

Vertraulichkeit

Hier werden die Daten bzw. Informationen vor dem Zugriff unbefugter Personen geschützt. Dies bedeutet, dass nur der Besitzer oder von ihm autorisierte Personen auf die Daten zugreifen können. Dieses Sicherheitsziel kann durch den Einsatz von Zutrittssicherungen, Zutrittsberechtigungen oder Verschlüsselungen bei der Datenübertragung erreicht werden.

Verfügbarkeit

Die Verfügbarkeit der Daten ist bei bedeutenden Geschäftsprozessen und Prozessen mit hohem IT-Einsatz von großer Wichtigkeit. Es muss garantiert werden, dass die Daten, Software und Hardware dem Nutzer zu geforderten Zeiten zur Verfügung stehen. Redundante Komponenten wie Standby-Systeme sowie der Einsatz von Backups oder Filtermechanismen können die Verfügbarkeit der Systeme erhöhen.

[1] Wikipedia (2021): Informationssicherheit, unter: https://de.wikipedia.org/wiki/Informationssicherheit

rockenstein AG · Internet-Service-Provider
Ohmstraße 12 · D-97076 Würzburg
Tel.: +49-931-299 344· Fax: +49-931-29934-99
info@rockenstein.de · www.rockenstein.de
Vorstand: Christoph Rockenstein
Aufsichtsrat: Rainer Rockenstein
AG Würzburg, HRB 6774
USt-IdNr. DE198235012

Integrität

Dieses Schutzziel stellt sicher, dass Daten bei der Speicherung oder Übertragung nicht geändert werden. Darunter versteht man aber auch, dass eine nicht autorisierte Änderung des Datensatzes erkannt werden kann. Diese Eigenschaft ist besonders bei Finanztransaktionen bedeutend. Physische Sicherheitsmaßnahmen oder Zugriffskontrollen können die Manipulation durch Dritte erschweren. Hierzu können digitale Signaturen oder Message Authentication Codes verwendet werden.

Die zu schützenden Daten können sich dabei in verschiedenen Zuständen befinden. „Data at Rest" bezeichnet Daten, die auf einer Festplatte, Laptop, Flash Drive oder an einem anderen Ort gespeichert sind. Bewegen sich die Daten aktiv von einem Ort zu einem anderen, werden diese also übertragen, nennt man sie „Data in Transit".

Sicherheitsmaßnahmen der Datenübertragung

	Data in Transit	Data at Rest
Vertraulichkeit	Asymmetrische Verschlüsselungsverfahren	Symmetrische Verschlüsselungsverfahren
Integrität	Signaturverfahren	Hashfunktionen, Rechteverwaltung
Verfügbarkeit	Redundanz	Redundanz

Der starke Anstieg der Cyber-Angriffe in den letzten Jahren weltweit[2] führte dazu, dass die Informationssicherheit immer mehr an Bedeutung gewinnt. Der Diebstahl von Daten ist längst keine Seltenheit mehr. Hacker verschaffen sich Zugang zu vermeintlich gesicherten (Kunden-)Daten.[3] Dies kann erheblichen Schaden anrichten, wenn es sich um sensible Daten kritischer Infrastrukturen handelt. Um sensible Daten vor Angriffen zu schützen, gibt es viele Maßnahmen, die bei der Datenübertragung sowie der Datenspeicherung realisiert werden können.

Vertraulichkeit

Für den Schutz des Sicherheitsziels Vertraulichkeit können bei der Datenübertragung asymmetrische Verschlüsselungsverfahren verwendet werden. Hierbei besitzen die Kommunikationsteilnehmer jeweils einen

[2] Vgl. PwC (2015): Anzahl der jährlichen Cyberangriffe weltweit in den Jahren 2009 bis 2015, unter: https://de.statista.com/statistik/daten/studie/348766/umfrage/jaehrlicheanzahl-von-internetangriffen-weltweit/
[3] Vgl. Tagesschau (2019): Nach Datendiebstahl: Festgenommener 20-Jähriger legt Geständnis ab, unter: https://www.tagesschau.de/multimedia/video/video-491621.html

rockenstein AG · Internet-Service-Provider
Ohmstraße 12 · D-97076 Würzburg
Tel.: +49-931-299 344 · Fax: +49-931-29934-99
info@rockenstein.de · www.rockenstein.de
Vorstand: Christoph Rockenstein
Aufsichtsrat: Rainer Rockenstein
AG Würzburg, HRB 6774
USt-IdNr. DE198235012

privaten und einen öffentlichen Schlüssel, auch Private und Public Key genannt. Für den Transfer der Daten verschlüsselt nun der Sender diese mit dem öffentlichen Schlüssel. Die Entschlüsselung auf der Empfängerseite findet jedoch nur mit dem dazugehörigen privaten Schlüssel statt. Dadurch kann eine sichere Datenübertragung vor allem in der digitalen Kommunikation, wie der Austausch von E-Mails, gewährleistet werden.

Um ruhende Daten vor Angriffen zu schützen und Zugriff nur autorisierten Personen zu gewährleisten, können symmetrische Verschlüsselungsverfahren verwendet werden. Hierbei gibt es nur einen Schlüssel zur Ver- und Entschlüsselung der Daten. So können sensible Datensätze auf eigenen Servern in Rechenzentren abgelegt werden und nur von Besitzern dieses geheimen Schlüssels dekodiert werden.

Integrität

Um bei der Datenübertragung das Sicherheitsziel der Integrität zu gewährleisten, können digitale Signaturverfahren, wie sie im SSL-Protokoll verwendet werden, eingesetzt werden. Hier signiert der Sender eine Nachricht mit einem geheimen Schlüssel und übermittelt die Nachricht an den Empfänger. Dieser prüft mithilfe eines öffentlichen Schlüssels, ob die Signatur zur Nachricht passt und die Nachricht unmanipuliert ist.

Integrität bei ruhenden Daten kann auch durch die Verwendung kryptographischer Hashfunktionen sichergestellt werden. Diese bilden als Einwegfunktion einen beliebigen Datensatz (Datei) auf einen Hashwert ab. Eine Änderung des Datensatzes führt immer auch zu einer Änderung des zugehörigen Hashwertes. Ein unveränderter Hashwert gilt deshalb als Garantie für einen unveränderten Datensatz.

Verfügbarkeit

Um die Verfügbarkeit sowohl von gespeicherten Daten als auch bei der Übertragung zu erhöhen ist eine redundante Infrastruktur hilfreich. Fällt nun ein System oder ein Server aus, kann dies durch die redundante Infrastruktur aufgefangen werden. Die rockenstein AG stellt ihren Kunden einen redundant aufgebauten hochverfügbaren Backbone sowie optional eine redundante Anbindung bis zum Kundenstandort zur Verfügung. Darüber hinaus bietet die rockenstein AG redundant angelegte Cloud-Systeme an. Diese sind so konstruiert, dass selbst bei einem Komplettausfall eines Servers alle darauf betriebenen Systeme weiterhin verfügbar sind.

Ohmstraße 12
97076 Würzburg
Tel.: +49 931 299 344
info@rockenstein.de
rockenstein.de

rockenstein AG · Internet-Service-Provider
Ohmstraße 12 · D-97076 Würzburg
Tel.: +49-931-299 344· Fax: +49-931-29934-99
info@rockenstein.de · www.rockenstein.de
Vorstand: Christoph Rockenstein
Aufsichtsrat: Rainer Rockenstein
AG Würzburg, HRB 6774
USt-IdNr. DE198235012