Vertraulichkeit

Aus Kastel

Begriff	Vertraulichkeit
Hauptverantwortlicher	Thomas Bräuchle
Definition	Ein System bewahrt Vertraulichkeit wenn es keine unautorisierte Informationsgewinnung ermöglicht.
Synonyme:	Geheimhaltung
Erläuterung	Aus juristischer Sicht meint Vertraulichkeit, dass nur befugt (autorisiert) auf Daten und Verfahren zugegriffen werden kann (§ 5 Abs. 1 Satz 2 Nr. 3 LDSG-SH), mithin also Informationen eines IT-Systems nur Befugten (Autorisierten) zugänglich sind.[1] Aus technischer Sicht definiert Vertraulichkeit genau das, was unter Zugriffsschutz verstanden wird. Der Unterschied zwischen diesen Begriffen besteht darin, dass Vertraulichkeit nur auf den lesenden Zugriff beschränkt ist, wohingegen Zugriffsschutz zusätzlich manipulativen Zugriff abdeckt. Wie stark hingegen der Vertraulichkeitsbegriff zu gewichten ist hängt davon ab, welche Informationsgewinnung autorisiert werden kann und welche nicht. Es stellt sich dann beispielsweise die Frage, ob eine Information über die Länge des Chiffrats erlangt werden darf.
Abgrenzung:	
Verwandte Begriffe	
Diskussion:	Nach Jürjens[2] existiert eine Definition, die einen Angreifer und dessen Fähigkeiten direkt einbezieht. Danach wird ein Datum d geleakt, wenn ein Angreifer existiert, der Datum d initial nicht kennt, und eine Eingabesequenz an das System existiert, so dass nach der Ausführung der Sequenz durch das System im Beisein des Angreifers, dieser das Datum d kennt. Ein System, das Datum d nicht leakt erhält die Vertraulichkeit von Datum d. Ein Alternativvorschlag nach Eckert[3] besagt, dass "das System (...) Vertraulichkeit gewährleistet, wenn es keine unautorisierte Informationsgewinnung ermöglicht." Diese Definition beschränkt sich nicht auf den Zugang zu Daten o.ä., sondern bezieht explizit auch die Verarbeitung von Daten durch einen Angreifer ein. Außerdem wird nach dieser Definition die Unmöglichkeit der Informationsgewinnung gefordert. Die Möglichkeit, Schwachpunkte auszunutzen, wird also auf das Angreifermodell ausgelagert. Diese Definition ist technisch auf verschiedenste Arten verfeinerbar, so dass verschiedene Methoden zur Durchsetzung, zum Nachweis oder zur Analyse realisiert werden können. Die Definition nach Eckert birgt jedoch gewisse Unsicherheiten bezüglich des Begriffs Information. Daher könnte wie bei dem Begriff der Integrität zwischen starker und schwacher Vertraulichkeit unterschieden werden. Demzufolge würde ein System schwache Vertraulichkeit bewahren, wenn es keine unautorisierte Datengewinnung ermöglicht. Starke Vertraulichkeit hingegen läge vor, wenn es keine unautorisierte Informationsgewinnung ermöglicht.
Beispiel:	
Quellen	1. ↑ Bedner, Mark, and Tobias Ackermann. "Schutzziele der IT-sicherheit." Datenschutz und Datensicherheit-DuD 34.5 (2010): 323ff. 2. ↑ Jan Jürjens. Secure systems development with UML. Springer, Berlin, 2005. 3. ↑ Claudia Eckert. IT-Sicherheit : Konzepte - Verfahren - Protokolle. Oldenbourg, München, 2012.

```
@article{bedner2010schutzziele,
  title={Schutzziele der IT-sicherheit},
  author={Bedner, Mark and Ackermann, Tobias},
  journal={Datenschutz und Datensicherheit-DuD},
  volume={34},
  number={5},
  pages={323ff},
  year={2010},
  publisher={Springer}
}
@book{jurjens2005secure,
  title={Secure systems development with UML},
  author={J{\"u}rjens, Jan},
  year={2005},
```

```
  publisher={Springer}
}
@book{eckert2013sicherheit,
  title={IT-Sicherheit: Konzepte-Verfahren-Protokolle},
  author={Eckert, Claudia},
  year={2013},
  publisher={Oldenbourg Wissenschaftsverlag}
}
```

Von „https://wiki.kastel.kit.edu/delmonte/Vertraulichkeit“
Kategorie: Begriff