Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Smart Data

Security-Eckpunkte für Plattformlösungen

Schutzbedarfsanalyse und Sicherheitskonzept

Bei der Nutzung von personenbezogenen und sensiblen Daten müssen diese, aber auch die zugrundeliegenden Systeme, durch ein entsprechendes Sicherheitskonzept geschützt werden. Vorgelagert wird eine Schutzbedarfsanalyse durchgeführt zur Systematisierung spezifischer Anforderungen an Sicherheitsziele wie Verfügbarkeit, Integrität und Vertraulichkeit. Für diese Ziele werden konkrete Maßnahmen im Sicherheitskonzept definiert. Das Sicherheitskonzept kann auf Basis des IT-Grundschutzes entwickelt und zertifiziert werden.[1] Hierfür steht der kostenfreie BSI-Standard 100-2 „IT-Grundschutz Vorgehensweise“ als Einstiegswerk zur Verfügung.[2] Zu diesem Zweck sollten technische und organisatorische Schutzprinzipien zur (Kommunikations- und Daten-)Verschlüsselung, Zugriffs- und Nutzungskontrolle, Authentifikation, Anonymisierung bzw. Pseudonymisierung sowie zuverlässigen Speicherung bei der Entwicklung digitaler Plattformlösungen berücksichtigt und implementiert werden. Dabei kommt den Sicherheitsrichtlinien eine besondere Rolle zu.[3] Eine anschließende Zertifizierung nach dem anerkannten Standard ISO/IEC 27001 lässt sich auf Basis des IT-Grundschutzes ebenfalls vornehmen. Ratsam ist zudem eine intensive Auseinandersetzung mit Konzepten des technischen Datenschutzes, wie Datensparsamkeit, Transparenz, Nichtverkettbarkeit/Zweckbindung sowie Nutzerrechte/Intervenierbarkeit.

Verschlüsselung und Datenaustausch

Zur Verschlüsselung von Daten sind der aktuelle Stand der Technik, Transportverschlüsselung mittels TLS 1.3 und Verschlüsselung zu persistierender Daten mit AES zu berücksichtigen.[4] Besondere Aufmerksamkeit sollte zudem möglichen Verbindungs- und Schnittstellen zum Datenaustausch gewidmet werden. Eine Anbindung an andere Teilnetze kann z. B. mittels einer verschlüsselten VPN-Verbindung geschützt werden. Wenn (auch öffentliche) Webanwendungen bzw. Web-Schnittstellen geplant sind, wird angeregt, die Open Web Application Security Project (OWASP) Top 10 Liste[5] sowie die OWASP Automated Threats for Web Applications[6] in eine umfassende Bedrohungsanalyse und das Sicherheitskonzept miteinzubeziehen.

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/profile/ profile.html;jsessionid=FAF8946937CB46F-3048984F5A8C5CCC7.1_cid351
2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile
3 https://www.secorvo.de/publikationen/sicherheitsrichtlinien-fox-jendrian-2009.pdf
4 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6
5 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
6 https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Smart Data

Datenzugriff und Authentifizierung

Bei schützenswerten Daten ist es ratsam, ein angemessenes Zugriffskontrollsystem zu implementieren. Dabei sollten möglichst erprobte und etablierte Standards Verwendung finden. Ein gängiges und weitverbreitetes Modell ist das rollenbasierte Zugriffskontrollsystem (RBAC). Das Authentifizierungskonzept kann zudem durch eine Multi-Faktor-Authentifizierung profitieren. Als technische Lösung eignet sich beispielsweise OpenID[7], ein dezentrales Authentifizierungssystem für webbasierte Dienste. Ein Standard zum Identitätsmanagement und Konzepten nach Stand der Technik findet sich in der ISO/IEC 24760.[8] Bei der Verarbeitung personenbezogener Daten muss die Anwendung der zehn Datenschutzprinzipien gemäß Artikel 5 der DS-GVO zu Tragen kommen.[9] Im Rahmen einer Schutzbedarfsanalyse und der Gewährleistung der Datenschutzprinzipien kann das Standard-Datenschutzmodell genutzt werden.[10]

Anonymisierung und Pseudonymisierung

Ist die Anonymisierung und/oder Pseudonymisierung von Daten notwendig, wird auf die Stellungnahme 5/2014 zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe hingewiesen, in deren Anhang sich auch ein Leitfaden zu Anonymisierungstechniken befindet.[11] Darüber sollte evaluiert werden, welche Anonymisierungsmethoden mit semantischen Sicherheitsgarantien[12] sich eignen und inwieweit sie Anforderungen erfüllen, die sich aus dem Datenschutz ergeben. Solche Anonymisierungsmethoden haben den Vorteil, dass ihre Sicherheitseigenschaften klar definiert sind und auch Schutz gegenüber noch unbekannten Angriffen bieten. Beachtet werden sollten bei der Anonymisierung und Pseudonymisierung bestehende Begriffe oder Verfahren aus dem Bereich Data Privacy (k-Anonymity, l-Diversity, t-Closeness, Differential Privacy).

Sicherheit in der Cloud

Bei der Nutzung von Cloud-Diensten zur Verarbeitung von Daten und vor allem bei der Entwicklung eigener Cloud-Lösungen sollte sich an dem BSI-Eckpunktepapier „Sicherheitsempfehlungen für Cloud-Computing Anbieter – Mindestanforderungen in der Informationssicherheit“ orientiert werden.[13] Weiterhin wird empfohlen, auf die Vorarbeiten und Ergebnisse des Trusted-Cloud-Technologieprogramms zurückzugreifen.[14] Mithilfe der dort erarbeiteten Charakteristika für vertrauenswürdige Cloud-Angebote ist eine Bewertung und Zertifizierung von Cloud-Service-Betreibern möglich. Entsteht im Projekt eine eigene Cloud-Lösung, besteht somit die Möglichkeit, die im Projekt erarbeitete Lösung mit dem Trusted-Cloud-Label zu zertifizieren und so ein höheres Vertrauen in das Angebot zu schaffen.

7 https://openid.net/
8 https://www.iso.org/standard/57914.html
9 Siehe dazu: Art. 5 DS-GVO (Grundsätze für die Verarbeitung personenbezogener Daten), via: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&qid=1481744755386&from=DE
10 https://datenschutzzentrum.de/sdm/
11 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf Die Stellungnahme bezieht sich auf die Rechtslage vor der DS-GVO, die jedoch in wesentlichen Aspekten der Anonymisierung an die Datenschutzrichtlinie anknüpft, weshalb insbesondere die technischen Aussagen übertragbar sind.
12 https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf
13 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Eckpunktepapier/ Eckpunktepapier_node.html
14 https://www.trusted-cloud.de/

Ansprechpartner im Smart-Data-Programm

PD Dr. Oliver Raabe und Manuela Wagner

Begleitforschung Smart Data
www.smart-data-programm.de

c/o FZI Forschungszentrum Informatik
Außenstelle Berlin
Friedrichstr. 60, 10117 Berlin
Mail: kontakt@smart-data-programm.de