1 Eigenschaften sicherer Software

Informationen und Daten sind im Bezug auf ihre wirtschaftliche Relevanz schützenswerte Güter. Der Zugriff auf Daten sollte daher beschränkt sein. Lediglich autorisierte Benutzer:Innen und Programme sollten auf Informationen zugreifen können. In der Literatur werden daher drei Schutzziele definiert, deren Einhaltung einen umfangreichen Schutz vor Angriffen von außerhalb des IT-Systems und innerhalb bieten. Ziel dieser Maßnahmen ist es vertrauliche Daten vor unbefugten Zugriff, sei es aus Datenschutzrechtlichen Gründen, Betreibsgeheimnissen zu schützen. Bei diesen Schutzzielen handelt es sich um Vertraulichkeit, Integrität und Verfügbarkeit. Aus diesen Zielen lassen sich noch drei erweiterte Schutzziele ableiten, Verbindlichkeit, Zurechenbarkeit und Authentizität, die zusammen mit den bereits Genannten in den Folgenden Kapiteln definiert werden [1]. Werden diese Schutzziele umgesetzt, kann ein verlässliches IT-System gewährleistet werden, dass von Bernhard Witt wie folgt charakterisiert wird: 'Unter Verlässlichkeit von IT-Systemen ist zu verstehen, dass keine unzulässige Beeinträchtigung der IT-Systeme, der gespeicherten Daten und der genutzten Funktionen bzw. Prozesse im Bestand, ihrer Nutzung oder ihrer Verfügbarkeit erfolgt'[2].

1.1 Schutzziel Vertraulichkeit

Vertraulichkeit (eng. confidality) beschreibt die Gewährleistung, dass die Daten des IT-Systems nur von befugten Nutzer interpretiert werden kann. Ihr Nachweis ist allerdings das Sicherheitskriterium der Verlässlichkeit, das am schlechtesten nachzuweisen ist. Denoch ist gerade dieses Kriterium sowohl zur Gewährleistung von Compliance, womit die Erfüllung der Verpflichtungen aus rechtlichen und organisatorischen Anforderungen gemeint ist, als auch zur Absicherung der Betriebs- und Geschäftsgeheimnisse essentiell. Ein entsprechender Informationsgewinn darf sich nur für die befugten Nutzer erschließen. Für Unbefugte müssen Daten (Nutzdaten, Passwortdaten, etc.) unzugänglich sein oder zumindest in nicht interpretierbarer Form vorliegen. Der Zugriffsschutz sollte dabei je nach Schutzwürdigkeit der Daten unterschiedlich ausfallen. Das zentrale Instrument zur Gewährleistung der Vertraulichkeit ist neben einem wirksamen Zugriffsschutz die Verschlüsselung von Daten. Zur Gewährleistung von Vertraulichkeit sind ebenfalls weitere Schutzziele aus der Kommunikationstechnik zu zählen. Darunter fallen die

Absicherung von Anonymität, Pseudonymität, Unbeobachtbarkeit und Verdecktheit. Da für diese Arbeit die Verschlüsselung der Daten ein größerer Wert zugeordnet wird, wird hier auf weitere Definitionen verzeichtet [2].

1.2 Schutzziel Integrität

Unter Integrität versteht man die Gewährleistung, dass Daten des IT-Systems nur durch befugte Nutzer verändert werden. Dadurch wird die Korrektheit der gespeicherten Daten und Informationen gewährleistet. Dies setzt also das Vorleigen originalgetreuer, unverfälschter und aktueller Daten voraus. Unbefugte Manipulation an Daten (Nutzdaten, Passwortdaten, etc.), sowie an ihrer technischen Darstellung müssen feststellbar sein. Die Integrität zielt also auf die Vollständigkeit des Datensatzes einserseits und auf die Konsistenz im Sinne einer hohen Datenqualität andererseits ab. Dies sicherzustellen ist eine wichtige Aufgabe der Wiederherstellung von Datenbeständen im Katastrophenfall und damit der Datensicherung. Entsprechende Back-Up Konzepte sind daher ein wichtiger Teil zur Gewährleistung der Integrität von Daten in IT-Systemen. Die handelsrechtliche wie auch steuerrechtliche Überprüfbarkeit von Unternehmensdaten verlangt neben der Existenz entsprechender Dokumente, auch ihre Orginalität, Unversehrtheit und Korrektheit, was durch Maßnahmen zur Integritätssicherung zu gewährleisten ist [2].

1.3 Schutzziel Verfügbarkeit

Zentral für die Gewährleistung von IT-Sicherheit ist die Verfügbarkeit, zumal eine Störung dieser Sicherheitsvorgabe als erstes Festgestellt werden kann und sich auf die anderen Sicherheitsvorgaben direkt auswirkt. Bernhard Witt liefert dabei folgende Definition für Verfügbarkeit (eng availability): 'Gewährleistung, dass das IT-System (für befugte Nutzer) zugänglich und funktionsfähig ist'. Unter Verfügbarkeit ist also zu verstehen, dass ein (von einer befugten Person oder durch einen befugten Prozess ausgelöster) Prozess in vorgesehener Weise, zum geplanten Zeitpunkt und im vorgegebenen Zeitrahmen ausgeführt wird. Dies ist nur dann möglich, wenn die zur Verarbeitung erforderlichen Ressourcen für die Verarbeitung erreichbar sind, genutzt werden können und vor Ausfällen und Verlust geschützt sind. Je wichtiger ein IT-System für ein Unternehmen oder Nutzer:In, desto höhere Verfügbarkeitsanforderungen sind an das System zu stellen [2].

1.4 Erweiterte Schutzziele

Neben den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit gibt es noch drei erweiterte Schutzziele. Zu ihnen zählen Verbindlichkeit, Zurechenbarkeit und Authentizität.Die ersten beiden Ziele ergänzen sich in sofern, dass unter Verbindlichkeit verstanden wird, dass ein Akteur seine Handlung innhalb des IT-Systems nicht abstreiten kann. Unter Zurechenbarkeit versteht man, dass jedem Akteur sein Handeln eindeutig zugeordnet werden kann. Wenn beide Eigenschaften erfüllt sind, können alle getätigten Handlungen innerhalb des Systems nachverfolgt und die handelnde Person erkannt werden. Also ist eine eindeutige Identifizierbarkeit von Akteuren gewährleistet [3]. Dies ist in sofern relevant, da Daten und Vorgänge gegenüber Dritten jederzeit rechtkräftig nachgewiesen werden können. Auserdem lassen sich somit die mithilfe des eingesetzten IT-Systems getätigten Aktionen gezielter rückgängig machen. Die Eigenschaft der Revisionefähigkeit wird somit gestärkt [2].
Als drittes erweitertes Schutzziel wird Authentizität verstanden (Echtheit). So wird die Frage geklärt, ob Informationen echt sind oder tatsächlich von der angegebenen Quelle stammen. Dieses Schutzziel hat zur Aufgabe die Vertrauenswürdigkeit des Urspungs von Informationen bewertbar zu machen [3]. Die Authentizität dient also der Unabstreitbarkeit der Zuordnung von Verantwortung. Erst, wenn eine Zurechnung glaubwürdig erfolgt, können rechtwirksame Folgen greifen. Dabei fordert die Nachweisbarkeit der Authentizität eine detaillierte Protokolierung [2].

1. Claudia Eckert: IT-Sicherheit. Konzepte – Verfahren – Protokolle. 2.
IT-Sicherheit kompakt und verständlich. Bernhard C. Witt 3. "https://www.dqs.de/blog/informationss
informationssicherheit-definition/"