**1 IT-Grundschutz – Basis für Informationssicherheit[[1]](#footnote-1)**

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Geschäftsprozesse und Fachaufgaben sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der sogar existenzbedrohend werden kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen. Mit dem IT-Grundschutz bietet das BSI eine praktikable Methode an, um die Informationen einer Institution angemessenen zu schützen. Die Kombination aus den IT-Grundschutz-Vorgehensweisen Basis-, Kern- und Standard-Absicherung sowie dem IT-Grundschutz-Kompendium bieten für unterschiedliche Einsatzumgebungen Sicherheitsanforderungen zum Aufbau eines ISMS (Informationssicherheits-Management-Systems) und somit für den sicheren Umgang mit Informationen.

Aufgrund der skizzierten Abhängigkeit steigt bei Sicherheitsvorfällen auch die Gefahr für Institutionen, einen Imageschaden zu erleiden. Die verarbeiteten Daten und Informationen müssen adäquat geschützt, Sicherheitsmaßnahmen sorgfältig geplant, umgesetzt und kontrolliert werden. Hierbei ist es aber wichtig, sich nicht nur auf die Sicherheit von IT-Systemen zu konzentrieren, da Informationssicherheit ganzheitlich betrachtet werden muss. Sie hängt auch stark von infrastrukturellen, organisatorischen und personellen Rahmenbedingungen ab. Die Sicherheit der Betriebsumgebung, die ausreichende Schulung der Mitarbeiter, die Verlässlichkeit von Dienstleistungen, der richtige Umgang mit zu schützenden Informationen und viele andere wichtige Aspekte dürfen auf keinen Fall vernachlässigt werden. Mängel im Bereich der Informationssicherheit können zu erheblichen Problemen führen.

Die potenziellen Schäden lassen sich verschiedenen Kategorien zuordnen:

**1. Verfügbarkeit**

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Verlust der Verfügbarkeit

Wenn grundlegende Informationen nicht vorhanden sind, fällt dies meistens schnell auf, vor allem, wenn Aufgaben ohne diese nicht weitergeführt werden können. Funktioniert ein IT-System nicht, können beispielsweise keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind nicht möglich, Produktionsprozesse stehen still. Auch wenn die Verfügbarkeit von bestimmten Informationen lediglich eingeschränkt ist, können die Geschäftsprozesse bzw. Fachaufgaben einer Institution beeinträchtigt werden.

**2. Vertraulichkeit**

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Verlust der Vertraulichkeit von Informationen

Jeder Bürger und jeder Kunde möchte, dass mit seinen personenbezogenen Daten vertraulich umgegangen wird. Jedes Unternehmen sollte wissen, dass interne, vertrauliche Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.

**3. Integrität**

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen“ angewendet. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Verlust der Integrität (Korrektheit) von Informationen

Gefälschte oder verfälschte Daten können beispielsweise zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen. Auch der Verlust der Authentizität (Echtheit und Überprüfbarkeit) hat, als ein Teilbereich der Integrität, eine hohe Bedeutung. Daten werden beispielsweise einer falschen Person zugeordnet. So können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die „digitale Identität“ wird gefälscht.

Aufgaben

1. Lesen Sie den Text und recherchieren Sie unbekannte Begriffe eigenständig.

*Partnerarbeit*

1. Klären Sie eventuelle Verständnisprobleme miteinander.
2. Erklären Sie Vertraulichkeit, Integrität und Verfügbarkeit sowie die Verstöße dagegen anhand eines Beispiele Ihrer Wahl (z.B. einer in Teams abgelegten Datei mit Schülernamen und entsprechenden Bildern).
3. Kategorisieren Sie die Schadenszenarien 1-4 aus der letzten Stunde (nächste Seite). Wählen sie zusätzlich ein eigenes Schadensszenario (5). Beschreiben Sie schließlich VIV (alle!) für die Szenarien 6 - 8.

|  |  |  |  |
| --- | --- | --- | --- |
| **Schadensszenarien** | **Vertraulichkeit** | **Integrität** | **Verfügbarkeit** |
| **1 – Verlust der Festplatte** |  |  |  |
| **2 – fremder Eingriff auf Festplatte** |  |  |  |
| **3 – Abgriff persönlicher Daten** |  |  |  |
| **4 – Malware auf der Festplatte** |  |  |  |
| **5 -** |  |  |  |
| **6 – In Amazon angemeldet bleiben an Schulrechner** |  |  |  |
| **7 – Handy verloren** |  |  |  |
| **8 – Source code von Programm gestohlen** |  |  |  |

1. Bundesamt für Sicherheit in der Informationstechnik – IT-Grundschutz-Kompendium, online unter:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT\_Grundschutz\_Kompendium\_Edition2021.pdf?\_\_blob=publicationFile&v=6, letzter Zugriff: 31.08.2021 [↑](#footnote-ref-1)