Schutzziele der Informationssicherheit

Was bedeutet Informationssicherheit

Aufgrund der hohen Bedeutung von Informationen als Unternehmenswerte sollte die Informationssicherheit als notwendige Managementaufgabe verstanden werden, um Datenverlust und Datenmissbrauch zu verhindern. Ziel der Informationssicherheit ist es, Risiken auf ein für die Organisation akzeptables Niveau zu minimieren.

Schutzziele der Informationssicherheit

Die drei primären Schutzziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Im Folgenden werden zunächst die Begriffe anhand der Definitionen des Bundesamts für Sicherheit in der Informationstechnik (BSI) erläutert. Im Anschluss folgt ein kurzes Praxisbeispiel zu jedem Begriff.

1. Vertraulichkeit

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

Beispiele für Vertrauliche Informationen sind Kundendaten, Patente oder Forschungsdaten. Ein besonderer Schutz der Vertraulichkeit besteht zudem bei der Verarbeitung von personenbezogenen Daten, der in der Datenschutzgrundverordnung (DSGVO) und im Bundesdatenschutzgesetz (BDSG) gesetzlich geregelt ist. In der Praxis besteht die Gefahr von Verstößen gegen die Vertraulichkeit, wenn z.B. Flipcharts und Whiteboards nach Besprechungen nicht gereinigt werden, oder Kundendaten in Büros mit Publikumsverkehr offen zugänglich sind. Um die Vertraulichkeit von Informationen sicherzustellen, muss klar festgelegt sein, wer in welcher Art und Weise berechtigt ist, auf diese Daten zuzugreifen.

2. 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. 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."

Integritätsverlust von Informationen kann durch unautorisiertes Ändern, Löschen oder Einfügen von Daten eintreten. Werden beispielsweise Messdaten von Medizingeräten manipuliert, können daraus gravierende Folgen für die Patienten entstehen.

3. 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."

Gute Beispiele für Verfügbarkeit sind die Anforderungen an Server, Netze und Rechenzentren, die oft vertraglich in Service Level Agreements geregelt sind. Dabei bedeutet Verfügbarkeit nicht, dass die Informationen permanent zugänglich sein müssen. Informationen für Gehaltsabrechnungen müssen bspw. lediglich im festgelegten Zeitraum der monatlichen Abrechnungen verfügbar sein, wohingegen die Verfügbarkeit der Plattform eines Onlinehändlers deutlich höher sein dürfte. Zur Verhinderung von Systemausfällen sollte daher eine Risikoanalyse erfolgen, in der die Ausfallwahrscheinlichkeit, die Ausfallzeit und das Schadenspotential der absolut notwendigen Systeme und Anwendungen betrachtet werden.

Erweiterte Schutzziele der Informationssicherheit

In bestimmten Zusammenhängen können noch zusätzliche Schutzziele definiert werden. Diese sind oft die Authentizität, Nichtabstreitbarkeit, Verbindlichkeit und Zuverlässigkeit.

Authentizität

„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen."

Dieses Schutzziel der Echtheit von Informationen ist wichtig, um die Vertrauenswürdigkeit des Ursprungs einer Information bewerten zu können.

Nichtabstreitbarkeit

„Bei der Nichtabstreitbarkeit liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten."

Verbindlichkeit

„Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann."

Ein Beispiel für die Schutzziele der Nichtabstreitbarkeit und der Verbindlichkeit ist das Identitätsmanagement von Organisationen. Dadurch können Handlungen immer eindeutigen Identitäten zugeordnet werden und nachvollziehbar und verbindlich Nutzern zugewiesen werden können, sodass sie auch nicht abgestritten werden können.

Zuverlässigkeit

Das Schutzziel der Zuverlässigkeit bezieht sich auf die technische Funktionsfähigkeit von IT-Systemen und Komponenten und kann daher in Szenarien hoher Abhängigkeit von IT-Systemen zusätzlich zum Schutzziel der Verfügbarkeit betrachtet werden.

Betrachtet man die Authentizität als Ergänzung der Integrität, so kann man die Sicherstellung der vier obigen Schutzziele mit dem Begriff **„VIVA-Prinzip"** bezeichnen.

Wie können Organisationen die Informationssicherheit erhöhen?

Zunächst muss das Bewusstsein dafür geschaffen werden, dass Informationssicherheit über technische Themen hinausgeht. Informationssicherheit ist ein übergreifendes Querschnittsthema, das organisatorische, technische, personelle und infrastrukturelle Aspekte umfasst. Das macht Informationssicherheit zu einer Aufgabe, die von der Unternehmensführung getragen und unterstützt werden muss.

Darüber hinaus muss jedes Unternehmen und jede Behörde ihre zentralen Informationswerte und Geschäftsprozesse kennen und deren Schutzbedarf und Risiken individuell bewerten, um die richtige Strategie zur Umsetzung der Informationssicherheit wählen zu können.

Schließlich sollte Informationssicherheit als Prozess und nicht als einmalige Aufgabe verstanden werden, da technischer Fortschritt und kurze Entwicklungszyklen informationsverarbeitender Systeme eine stetige Überprüfung und Verbesserung der Sicherheitsmaßnahmen erfordern. Dies kann am besten durch Implementierung eines ganzheitlichen Managementsystems der Informationssicherheit erreicht werden.