4 IT-Sicherheit

Bei der Nutzung von Internetdiensten, welcher Art auch immer, möchten wir, dass verantwortungsvoll mit unseren Daten umgegangen wird.
Allgemein gesprochen wollen wir, dass unsere Daten sicher sind und der Internetdienst bestimmte sich an Sicherheitsvorgaben hält.

4.1 Sicherheitsziele

Um diese Sicherheitsvorgaben zu vereinheitlichen, wurden die nachfolgenden Sicherheitsziele definiert.
Im Nachfolgenden sind diese am Beispiel *Online-Banking* verdeutlicht.

Authentizität

Instanz-Authentizität: Die Kommunikationspartner (Nutzer und Bank) sind davon überzeugt, dass ihr jeweiliges Gegenüber tatsächlich jene Partei ist, die sie vorgibt zu sein.

Datenursprungs-Authentizität: Die Kommunikationspartner können sicher sein, dass die empfangenen Nachrichten tatsächlich vom "erwarteten" Gegenüber stammen.

Integrität Die Nachrichten werden während der Übertragung nicht unautorisiert modifiziert, bspw. Ändern des Überweisungsbetrags.

Vertraulichkeit Keine dritte unautorisierte Partei kann die ausgetauschten Nachrichten, bspw. den Kontostand lesen.

Verfügbarkeit Die Online-Banking-Seite ist für autorisierte Benutzer "immer" erreichbar und erfüllt die vorgesehene Funktion.

Verbindlichkeit Keine der beiden Parteien kann im Nachhinein eine durchgeführte Transaktion abstreiten, bspw. eine durchgeführte Überweisung.

Anonymität Die Bank kann einen einzelnen Kunden unter der Menge der Kunden nicht eindeutig identifizieren.

Pseudonymität Der Kunde tritt unter einem Identifikator (ungleich Namen) gegenüber der Bank auf und die Bank kann - ohne die Kenntnis der Zuordnungsvorschrift mittels derer personenbezogene Daten verändert wurden - den Identifikator nicht mehr dem Kunden eindeutig zuordnen.

4.2 Angriffe

Wenn man an Sicherheit und die eigenen Daten denkt, so geht damit automatisch auch die Angst vor Angriffen auf diese Daten einher.
Bei solchen Angriffen sollte zwischen **aktiven** und **passiven** Angriffen unterscheiden.

4.2.1 Passiver Angriff

Ein passiver Angriff ist in der Regel schwer zu erkennen, da keine Daten modifiziert werden. Bei einem solchen Angriff ist weder dem Sender noch Empfänger ersichtlich, dass seine Daten mitgelesen werden.
Ziel eines solchen Angriffs ist das unbemerkte Sammeln von Daten ohne eine Interaktion zwischen Angreifer und Opfer.

4.2.2 Aktiver Angriff

Auch bei aktiven Angriffen ist das Ziel das Abgreifen und Sammeln von Daten. Hierbei besteht aber die Möglichkeit, dass der Angriff auf Seiten des Senders oder Empfängers erkannt wird.

4.2.3 Angriffsbeispiele

Abhören (*passiver Angriff*): Ziel ist eine unautorisierte Kenntnisnahme von Information.

Verkehrsanalyse (*passiver Angriff*): Ziel ist das Herausfinden von Kommunikationsbeziehungen. Also beispielsweise wer kommuniziert wie lange mit wem.

Maskerade (*aktiver Angriff*): Bei einem solchen Angriff verschafft sich der Angreifer (ohne Zugriffsberechtigung), indem er sich als Nutzer (mit Zugriffsberechtigung) unautorisiert Zugriff zu Diensten.

Wiederholungs-Angriff (*aktiver Angriff*): Hierbei werden passiv mitgehörte Nachrichten in das System wieder eingespielt um dadurch unautorisiert eine Dienstnutzungserlaubnis zu erlangen.

Modifikation (*aktiver Angriff*): Das Ziel dieses Angriffes ist die Veränderung von legitimen Nachrichten (bzw. Teilen davon).
Das Zurückhalten von Nachrichten oder auch das Umordnen des Verkehrsflusses kann hierzu zählen.

Denial of Service (*aktiver Angriff*): Bei einem solchen Angriff wird durch eine Vielzahl von parallel abgesetzten Anfragen an einen Service (z.B. eine Website) ebendieser nicht mehr verfügbar.