
Als offenes Netzwerk bietet das Internet Angreifern leichte Beute

2

Jeder kennt die Bedrohungen im Internet – Hackerangriffe, Identitätsklau oder Schnüffeleien – als dunkle Kehrseite der Dank des Internets entstandenen neuen digitalen Welt. Die wunderbar vereinfachten Kommunikationsmöglichkeiten, die das Internet bietet, haben in historisch kürzester Zeit alle Bereiche unseres Lebens und der menschlichen Gesellschaft erobert und zu einem unvorstellbar großen digitalen Datenschatz geführt, der auf mit dem Internet verbundenen Server-Rechnern gelagert für jeden Internetnutzer erreichbar ist. Während man diese Rechner weitgehend vor fremdem Zugriff schützen kann, bieten sich doch für Angreifer immer wieder Zugriffsmöglichkeiten, nämlich immer dann, wenn die Daten zwischen diesen Rechnern über das jedermann zugängliche offene Internet ausgetauscht werden (siehe Abb. 2.1).

Das weltweite Internet ist vom Funktionsprinzip her ein offenes Computernetzwerk: Jeder Interessierte kann im Detail Kenntnis erlangen vom Aufbau des Internets und der Protokolle, vermittels derer die Kommunikation im Internet technisch bewältigt wird. Tatsächlich war diese Offenheit – Kenntnisse über die Funktionsweise und Anschlussmöglichkeit für jedermann – die Voraussetzung für den Siegeszug des Internets, und warum es sich in so kurzer Zeit überhaupt so rasant verbreiten konnte. Prinzipiell jeder, der sich mit dem Internet verbindet, kann mit entsprechenden technischen Kenntnissen und Werkzeugen auf potenziell alle im Internet kommunizierten Daten und Nachrichten zugreifen; das Internet ist nicht beschränkt auf einen vertrauenswürdigen Personenkreis.

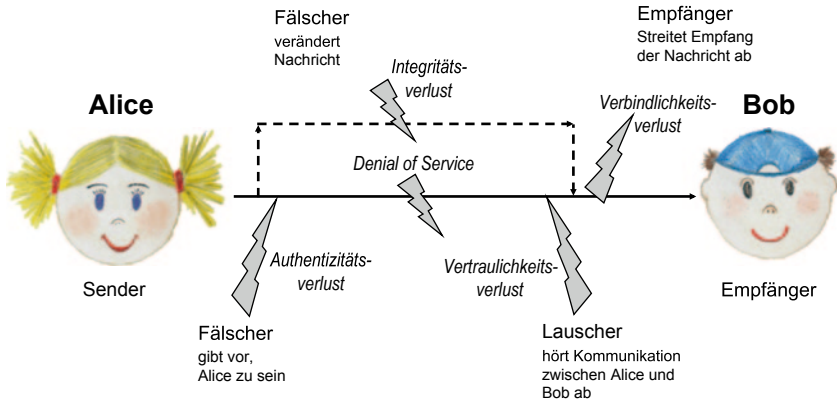


Abb. 2.1 Unterschiedliche Arten der Bedrohung in Kommunikationsnetzen

Bevor wir im Folgenden auf den Schutz der Kommunikation in offenen Netzen wie dem Internet eingehen und die dafür entwickelten kryptografischen Techniken und Verfahren vorstellen wollen, müssen wir zunächst einmal wichtige Eigenschaften und Aspekte zusammentragen, die für die Gewährleistung einer sicheren Kommunikation im Internet von Bedeutung sind.

Sicherheit und Vertrauen im Internet

Eine technische Perspektive

Meinel, C.; Sack, H.

2014, VIII, 48 S. 15 Abb., Softcover

ISBN: 978-3-658-04833-4