Kryptografie für Dummies

Symmetrische und asymmetrische Verschlüsselung verstehen

IN DIESEM KAPITEL

- Sichere Webseiten mit https
- Was ist ein Zertifikat?
- Verschlüsselung der übermittelten Daten

Kapitel 1
Sicherheit in Zeiten des Internet

Wussten Sie, dass nahezu das gesamte, in diesem Buch festgehaltene Wissen aufgeboten wird, wenn Sie im Internet eine Banküberweisung machen?

Kryptografische Verfahren sorgen dafür, dass dieser Vorgang sicher über die Bühne geht, genau so wie gewünscht, ohne unerwünschte Einwirkungen von Dritten, ohne Fälschen, Tricksen, Täuschen. Und das ist gar nicht so einfach, denn der Einfallsreichtum gewisser interessierter Kreise ist groß, gerade wenn es ums Geld geht.

Wenn Sie mit dem Firefox-Webbrowser die Webseite einer Bank aufrufen, wird das gesicherte Internet-Protokoll https verwendet. Sie erkennen dies an dem Schloss-Symbol in der Adresszeile des Webbrowsers (Abbildung 1.1):

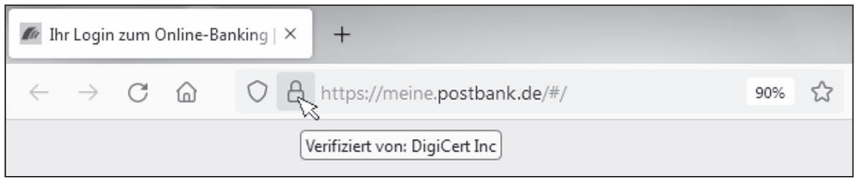

Abbildung 1.1: Adresszeile einer Bank-Webseite

Das normale Internet-Protokoll http (*Hypertext Transfer Protocol*) ist nicht gesichert. Aber wodurch unterscheidet sich https davon (das s steht für *secure* – sicher)? Es sorgt für die Authentizität der Datenverbindung sowie für die Vertraulichkeit und Integrität der Datenübertragung. Was diese Begriffe bedeuten, erfahren Sie im Folgenden.

Authentizität

Zunächst einmal gewährleistet https, dass Sie auch wirklich die Webseite der Bank aufrufen und nicht eine andere, gefälschte Seite. Dies ist wichtig, denn wenn Sie Ihre Bank-Zugangsdaten und Ihr Passwort auf einer gefälschten Seite eingeben, gelangen diese in die falschen Hände. Sie kennen Warnhinweise wie den folgenden:

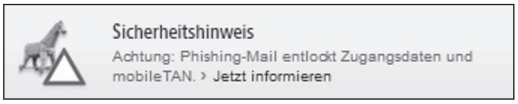

Abbildung 1.2: Warnhinweis: Phishing-Mails im Umlauf

Phishing ist eine Wortprägung für *password fishing*. Betrüger halten bildlich gesprochen eine Angel ins Wasser und warten darauf, dass jemand so arglos ist und anbeißt.

Wenn Sie eine E-Mail bekommen, in der Sie darauf hingewiesen werden, dass Ihre Bank-Zugangsdaten in Kürze ablaufen – was machen Sie? Klicken Sie auf den angebotenen Link »Jetzt Zugangsdaten aktualisieren«? Auch wenn Sie grundsätzlich an das Gute im Menschen glauben, sollten Sie in diesem Fall nicht arglos anbeißen.

Sie landen nämlich auf einer gefälschten Webseite, die der echten Bank-Webseite nachempfunden ist. Dort sollen Sie Ihre Zugangsdaten und Ihr Passwort eingeben. Jeder kann eine Webseite so gestalten, dass sie wie die echte Bank-Webseite aussieht.

Wenn Sie Zweifel haben, ob Sie wirklich auf der echten Bank-Webseite gelandet sind, dann achten Sie zunächst darauf, ob sich in der Adresszeile des Webbrowsers ein Schloss-Symbol befindet. Das Schloss-Symbol deutet darauf hin, dass sich der Webserver, von dem Sie die Webseite bekommen, gegenüber Ihrem Webbrowser *authentifiziert* hat. Wie macht er das? Der Webserver authentifiziert sich mittels eines Zertifikats.

Zertifikat

Ein Zertifikat ist vergleichbar mit einem Ausweis. Mithilfe Ihres Personalausweises können Sie sich gegenüber Dritten authentifizieren – Sie können beweisen, dass Sie derjenige sind, für den Sie sich ausgeben. Der Personalausweis stellt die Verbindung zwischen Ihnen (durch das Foto identifiziert) und Ihrem Namen her. Und den Personalausweis haben Sie sich nicht selbst hergestellt, sondern Sie haben ihn von einer vertrauenswürdigen Behörde ausgestellt bekommen.

In ähnlicher Weise stellt ein Zertifikat die Verbindung zwischen einer Webseite und dem Eigentümer der Webseite her. Wie ein Ausweis, so muss auch das Zertifikat von einer vertrauenswürdigen Instanz ausgestellt sein. An einem gültigen Zertifikat erkennen Sie, dass die Webseite diejenige ist, für die sie sich ausgibt – also nicht gefälscht ist.

Ob das Zertifikat gültig ist, müssen Sie im Prinzip überprüfen. Schließlich kann sich auch der Eigentümer einer gefälschten Webseite ein Zertifikat ausstellen lassen – er kann sich jedoch kein Zertifikat mit dem Namen Ihrer Bank ausstellen lassen. Für Sie ist wichtig, dass Sie zwei Dinge überprüfen:

- ✔ ob das Schloss-Symbol in der Adresszeile erscheint,
- ✔ ob beim Klicken auf das Schloss-Symbol der Name Ihrer Bank erscheint.

Wichtig ist auch noch, dass das Zertifikat von einer vertrauenswürdigen Instanz ausgestellt worden ist. Dies aber prüft der Webbrowser für Sie. Er kennt alle vertrauenswürdigen Instanzen, und wenn er eine nicht kennt, prüft er, ob diese ihrerseits ein Zertifikat einer vertrauenswürdigen Instanz besitzt, die er kennt.

Beim Firefox-Webbrowser erhalten Sie genauere Informationen über das Zertifikat, wenn Sie auf das Schloss-Symbol klicken und dann noch einmal auf den nach rechts weisenden Pfeil in dem erscheinenden Hinweis (Abbildung 1.3 und 1.4). Dort ist auch die vertrauenswürdige Instanz genannt, in diesem Fall die DigiCert Inc.

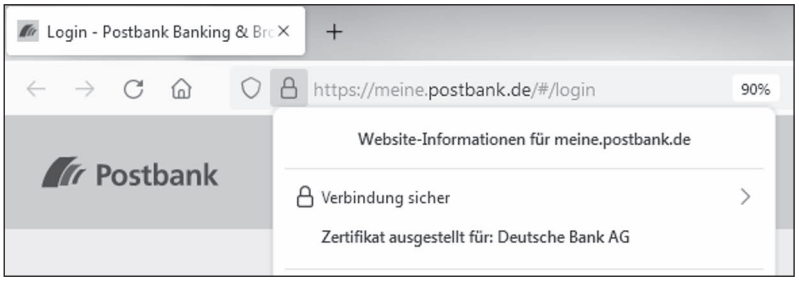

Abbildung 1.3: Eigentümer der Webseite

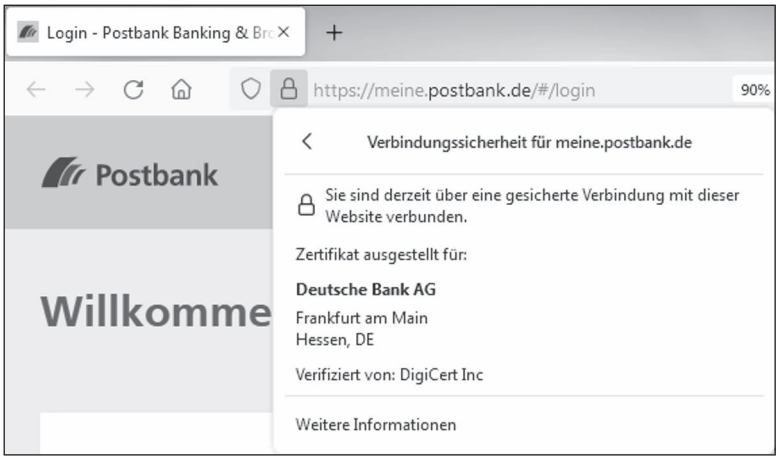

Abbildung 1.4: Webseiten-Sicherheitsinformation

Vertraulichkeit und Integrität

Das Internet-Protokoll https sorgt nicht nur für die Authentizität der Datenverbindung, sondern auch für Vertraulichkeit und Integrität der übermittelten Daten. Was bedeutet das?

Wenn Sie (wie früher) einen Brief mit der Post versenden, möchten Sie ja, dass nur der Empfänger den Brief liest. Deswegen stecken Sie den Brief in einen Briefumschlag und verschließen ihn. Denn Sie wissen, dass der Brief eine ganze Reihe von Stationen durchläuft, bevor er beim Empfänger ankommt – von demjenigen, der den Briefkasten ausleert über diverse Verteilzentren bis hin zum Briefträger, der den Brief zustellt.

Weil der Brief in einem verschlossenen Umschlag steckt, kann ihn niemand auf diesem Weg zum Empfänger lesen. Sie haben damit die *Vertraulichkeit* des Inhalts erreicht.

Sie erreichen mit dem Umschlag aber noch mehr: nämlich dass der Inhalt auf dem Weg zum Empfänger nicht verändert wird. Wer sollte daran Interesse haben? Nun, wenn der Inhalt des Umschlags aus einer Glückwunschkarte zum Geburtstag und einem 20-Euro-Schein besteht, gibt es manchmal durchaus Interessierte, die den Inhalt verändern möchten …

Wenn der Brief jedoch unversehrt beim Empfänger ankommt, kann dieser davon ausgehen, dass am Inhalt des Briefes nichts verändert worden ist – die *Integrität* des Inhalts ist damit erreicht.

Wie Sie wissen, werden auch im Internet die Datenpakete über eine Vielzahl von Stationen (Server und Router) geleitet, bis sie beim Empfänger ankommen – jede Menge Gelegenheiten, Nachrichten abzufangen, zu lesen und sogar zu verändern. Es geht also auch hier darum, Vertraulichkeit und Integrität der Nachricht zu erzielen. Beim Standardprotokoll http ist dies nicht gewährleistet; das Sicherheitsprotokoll https erreicht dagegen beides durch Verschlüsselung der Nachricht.

Der Sender verschlüsselt die Nachricht – er codiert die Nachricht in der Weise, dass sie für Dritte unleserlich ist. Nur der berechtigte Empfänger kann die Nachricht wieder entschlüsseln und anschließend lesen. Der Empfänger braucht zum Entschlüsseln eine geheime Zusatzinformation, einen Schlüssel. Dieser Schlüssel muss zu dem entsprechenden Schlüssel passen, mit dem der Sender die Nachricht verschlüsselt hat. Durch Verschlüsseln wird die *Vertraulichkeit* der Nachricht gewahrt.

Aber auch ein Verändern der Nachricht muss verhindert werden. Dies wird dadurch erreicht, dass von der Nachricht eine Art Fingerabdruck gewonnen wird und dieser mitverschlüsselt wird. Jede Veränderung an der verschlüsselten Nachricht führt dazu, dass die Nachricht und ihr Fingerabdruck nicht mehr zueinander passen. Der Empfänger bemerkt dies nach dem Entschlüsseln. Auf diese Weise wird die *Integrität* der Nachricht gewahrt.

Sicher surfen mit https

Das sichere Internet-Protokoll https sorgt somit dafür, dass die folgenden Sicherheitsziele eingehalten werden:

- ✔ Vertraulichkeit: Nur der berechtigte Empfänger kann die Nachricht lesen.
- ✔ Integrität: Der Empfänger kann feststellen, ob die Nachricht nach dem Absenden verändert worden ist.
- ✔ Authentizität: Der Empfänger kann feststellen, wer der Absender der Nachricht ist.

Wenn Sie in dem Info-Fenster aus Abbildung 1.4 unten auf »Weitere Informationen« klicken, erhalten Sie das in Abbildung 1.5 dargestellte Formular mit weiteren Informationen zur Sicherheit der Webseite.

Abbildung 1.5: Weitere Informationen zur Verschlüsselung

Im unteren Bereich unter »Technische Details« ist eine Information über die Verschlüsselung angegeben, ein Code, in dem die verwendeten Sicherheitsverfahren aufgelistet sind:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```

Jetzt, da Sie noch am Anfang dieses Buches sind, wird Ihnen nur das englische Wort `WITH` etwas sagen.

Aber nach und nach, während Sie dieses Buch lesen, kommen Sie auch der Bedeutung der drei bis sechs Zeichen langen Abkürzungen auf die Spur – und nicht nur das, sondern Sie lernen,

- ✔ welche Sicherheitsverfahren sich dahinter verbergen,
- ✔ wie diese funktionieren,
- ✔ wozu sie dienen und
- ✔ wie sicher sie sind.

Zum Schluss, in Kapitel 27, finden Sie zusammenfassend noch einmal die Auflösung, was dieser kryptisch anmutende Code bedeutet …

Ein Hinweis noch: Gegenüber der ersten Auflage dieses Buches von 2018 hat sich die Darstellung des Internet-Browsers Firefox geändert, ebenso die Zertifizierungsagentur der Postbank und auch das verwendete Sicherheitsverfahren. Die Änderungen sind aber nicht grundsätzlicher Art.

Seien Sie also nicht überrascht, wenn es zukünftig erneute Änderungen gibt, wenn vielleicht die Bildschirmdarstellung anders aussieht als in den vorstehenden Abbildungen oder wenn möglicherweise im Sicherheitsverfahren eine andere Schlüssellänge verwendet wird.