## Gefahren bei der Kommunikation über das Internet erkennen

In diesem Lernschritt werden die Schülerinnen und Schüler **in einer fiktiven Situation verschiedene reale Gefahren** der Kommunikation im Internet **erleben**. Dazu senden sie sich – wie bereits im Lernschritt zur Rekonstruktion der Protokolle SMTP und POP3 – fiktive Nachrichten über einen auf dem Lehrerrechner (oder einem anderen Rechner mit angeschlossenem Projektor) E-Mail-Server.

Um einen „man-in-the-middle"-Angriff realistisch demonstrieren zu können wird empfohlen, einen Standardrechner als Vermittlungsrechner (Router) umzubauen (siehe separate Anleitung „Einen Windows-Rechner zum Router machen"). Alternativ kann ein ähnlicher Angriff auf dem Lehrerrechner simuliert werden, nur ist die Trennung zwischen den Rollen Kommunikations-infrastruktur und Diensterbringer dann nicht mehr deutlich erkennbar. In jedem Fall reichen die Mittel von *Socket Sniff* nicht aus, um Passwörter, die Schülerinnen und Schüler für die fiktiven E-Mail-Konten nutzern, auszuspähen, da der E-Mail-Server *Hamster* diese ausblendet und eine Aufzeichnung der Kommunikation des Hamsters mit *Socket Sniff* nicht möglich scheint. Es wird daher empfohlen, dass Lehrende auf die Verwendung von *Wireshark* zurückgreifen.

### Vorbereitung

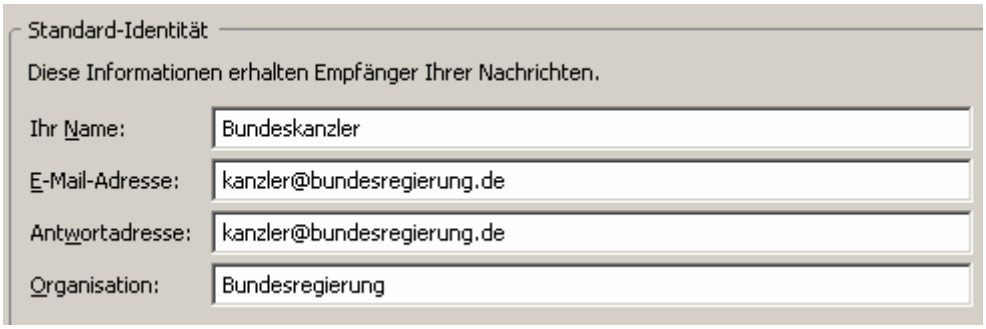
Vor Unterricht sollten Lehrende ggf. den Router vorbereiten (siehe separate Anleitung) und das spätere Versenden einer E-Mail mit gefälschten Absender-Angaben wie folgt vorbereiten:

a. Einen weiteren Schülerrechner starten und sich an dem Rechner anmelden.

b. Einen E-Mail-Client (z. B. *Thunderbird*) starten und für einen gültigen Benutzer des E-Mail-Servers einrichten (siehe Anleitung „E-Mail-Client *Thunderbird* einrichten" ).

c. Die Einstellungen zur Identität abändern:

- Menu „Extras > Konten" wählen.
- Die Angaben zur Standardidentität ändern, z. B.:




d. Eine E-Mail mit einer vermeintlich vertrauensvollen Information (z. B. Ankündigung einer bevorstehenden Privatisierung eines Staatsunternehmens mit Empfehlung eines Aktienkaufs vor Veröffentlichung des Vorhabens) an den Kurs schreiben und speichern (NOCH NICHT SENDEN – die Postfächer werden ja erst noch erstellt!). Dabei können als Email-Adressen jeweils <vornameDesSchuelers>@<RechnernameDesServers> angenommen werden.

## Durchführung

Das folgende **Szenario** lässt sich in ca. 45 Minuten durchspielen. Für eine Sicherung der Sicherheitsanforderungen an Kommunikation Vertraulichkeit, Integrität und Authentizität ist zusätzliche Zeit zu veranschlagen.

1. Benutzer für die Kursteilnehmer neu einrichten, dabei sollten die Schüler ihre Passwörter selbst eingeben (z. B. durch Herumreichen der Tastatur) – die Schülerinnen und Schüler sollten zuvor darauf hingewiesen werden, nicht Passwörter zu wählen, die sie auch für andere Zugänge nutzen. **Warum?** Die Passwörter werden ja später in den POP3-Nachrichten ausgelesen – das wiederum den Schülerinnen und Schüler noch nicht sagen!

**Vortäuschen einer falschen Identität auf Client-Seite**

2. Die Schülerinnen und Schüler auffordern, die Einstellungen ihrer E-Mail-Clients ggf. anzupassen und sich einige E-Mails zu schicken.

    a. Dabei die unter falscher Identität erstellte E-Mail an den Kurs versenden.

    b. Anschließend mit *Wireshark* auf dem „Router“ das Passwort eines Schülers „abfangen“.

3. Schülerinnen und Schüler im Plenum versammeln und nach erhaltenen E-Mails befragen („Hat alles geklappt?“, „Irgendwelche Probleme oder Unregelmäßigkeiten?“).

    a. Die offensichtlich unautorisierte E-Mail wird zum Anlass genommen, festzustellen: „Hier passieren Dinge, die so nicht passieren sollten!“

    b. Vorschau: „Ich werde jetzt verschiedene Dinge machen.“

    c. Beobachtungsauftrag: „Notiert:
    Welche Gefahren bei der Kommunikation über das Internet lassen sich beobachten?“

4. [Bildschirmprojektion des vorbereiteten Schülerrechners]
    Die Einstellungen zur falschen Identität zeigen (siehe Vorbereitung Punkt 3.c).

    a. „Wie lässt sich feststellen, dass es sich um eine falsche Identität handelt?“
    [unglaubwürdig, unpersönlich: der Verfasser weiß nichts über mich.]
    „Ja, besser wäre, ich wüsste mehr über die Benutzer der Postfächer ...“

**Mitlesen vertraulicher Informationen auf dem Kommunikationsweg**

    b. Ein weiteres Konto mit den Benutzerdaten des Schülers, dessen Passwort Sie unter Punkt 2.b ermittelt haben, einrichten, E-Mails anzeigen lassen und eine sehr „unhöfliche“ Antwort verfassen.
    “Welche Folgen könnte mein Handeln haben?“
    [Streit, der Empfänger nimmt die Nachricht ernst]
    “Wie könnte ich auf das Passwort gekommen sein?“
    [Verbindung abgehört ...]

    c. [Bildschirmprojektion des „Routers“]
    Das Passwort im Protokoll von *Wireshark* zeigen.

**Manipulation auf dem E-Mail-Server**

5. [Bildschirmprojektion des „Servers“]

    a. Einen Schüler auffordern, sich mit einem anderen per Email zu verabreden.

    b. Die entstandene .msg-Datei im Ordner Mails\<benutzername> in einem Texteditor öffnen und Zeit und Ort der Verabredung ändern.

    c. Den Empfänger auffordern bitten, sein Postfach auf neue E-Mails zu prüfen.
    “Was machst Du zum verabredeten Termin?“
    [Ich stehe am falschen Ort.]
    “Welche Folgen könnte mein Handeln haben?“
    [Streit, der Empfänger glaubt nicht an eine Manipulation]
    “Wenn sich alle Mitarbeiter des E-Mail-Servers korrekt verhalten – ist dann eine Manipulation ausgeschlossen?“
    [Der Server kann von Fremden gehackt werden.]

**Ergebnissicherung**

6. Abschließend sollten die konkreten Beobachtungen verallgemeinert werden.

    a. „Was konntet Ihr beobachten?“ Dabei an der Tafele sammeln:

    - **Nachrichten mitlesen**
    - **Nachrichten verändern**
    - **Nachrichten unter falscher Identität verfassen**

    b. „Was sollte man also sicherstellen?“ Dabei an der Tafele ergänzen:

    - **Keiner kann** Nachrichten mitlesen**.**
    - **Keiner kann** Nachrichten verändern**.**
    - **Keiner kann** Nachrichten unter falscher Identität verfassen**.**

    c. „Dafür hat man auch Begriffe gefunden.“ An der Tafele ergänzen:

**<u>Anforderungen an eine sichere Kommunikation:</u>**

- **Vertraulichkeit:** Keiner kann Nachrichten mitlesen.
- **Integrität:** Keiner kann Nachrichten verändern.
- **Authentizität:** Keiner kann Nachrichten unter falscher Identität verfassen.

**Vorschau:** „Wir werden zunächst untersuchen, wie sich Vertraulichkeit herstellen lässt! Dieses Problem gibt es nicht erst, seitdem es Computer gibt, die Geheimhaltung von Nachrichten war schon vor tausenden Jahren ein brisantes Thema.“