Maßnahmen zur Datensicherheit

Wiederholung von Grundlagen der Kommunikation im Internet (vgl. Lerninhalte 1.4-04, S. 2)

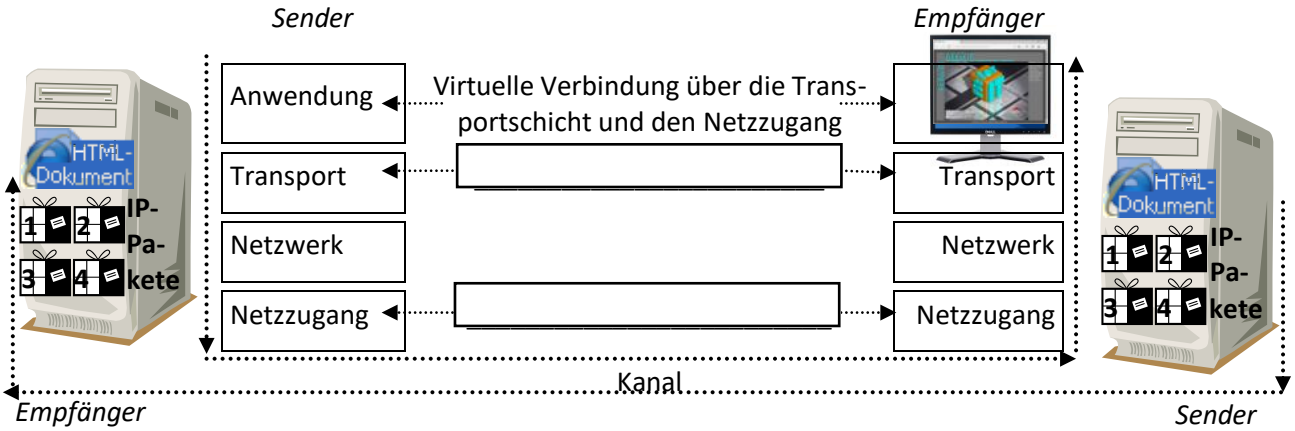
Die wichtigste Maßnahme zur Datensicherheit ist die **verschlüsselte Kommunikation**. Dadurch kann ein Unbefugter die gesendeten Daten nicht ohne Weiteres lesen.

1. Was versteht man unter einem **Protokoll**? Nenne ein grundlegendes Protokoll zur Kommunikation im Internet.

   Ergänze:

   - Ein **Host** ist ein Computer, der _____
   - Das Computerprogramm, das den Dienst anbietet, _____ wobei man oft auch das Gerät als Server bezeichnet, auf dem das Programm ausgeführt wird.
   - Ein **Client** ist ein Computerprogramm auf einem Gerät in einem Netzwerk, das _____ Auch das Gerät, das Dienste nutzt, nennt man oft Client.

2. Ergänze: Der Sender zerlegt die Daten in _____ und übermittelt sie zum Empfänger. **IP** ist die Abkürzung für **I**nternet **P**rotocol.



- Indem Nachrichten hin und her gesendet werden, tauschen die beiden Kommunikationspartner immer wieder die Rollen (Sender/Empfänger).
- Die eigentliche Kommunikation findet über die **Transport**schicht und den **Netzzugang** statt, weshalb diese Verbindungen auch *Ende-zu-Ende* bzw. *Punkt-zu-Punkt* genannt werden.
- Die Darstellung der Daten, z. B. einer HTML-Seite, findet in der **Anwendung**sschicht statt.

➢ Das grundlegende Protokoll zur Übermittlung von Webseiten auf der Anwendungsschicht ist **HTTP** (**H**yper**t**ext **T**ransfer **P**rotocol).

➢ Bei **HTTPS** steht das **S** für **S**ecure. Man kann es frei mit „sicheres Hypertext-Übertragungsprotokoll“ übersetzen. Bei Verwendung von HTTPS werden die Daten zwischen der Anwendungsschicht und der Transportschicht **verschlüsselt**.

Damit das funktioniert, vereinbaren die beiden Kommunikationspartner zu Beginn ihrer Sitzung einen Schlüssel auf der Basis eines Verschlüsselungsverfahrens.

3. Rufe einen Onlinedienst wie z. B. einen Webshop auf, bei dem eine sichere Verbindung hergestellt wird. Ob die Verbindung verschlüsselt ist, erkennst du an dem HTTPS und dem Schlosssymbol in der Adresszeile.

   Suche in dem Internetauftritt des Anbieters nach Informationen zu den verwendeten Verfahren zur Verschlüsselung. Notiere die Ergebnisse.
   Hinweis: Eine Website sollte einen Link *Datenschutz* auf der Startseite enthalten.

   Beispiel:

   Ihre Daten werden immer SSL-verschlüsselt übermittelt.

   Diese Aussage ist etwa genauso informativ wie die Aussage “die Sonne scheint” auf die Anfrage, ob es kalt oder warm ist. Denn es kann warm sein, wenn die Sonne scheint. Genauso gut kann es aber auch kalt sein, wenn die Sonne scheint. Eins ist sicher: Es regnet wenigstens wahrscheinlich nicht.

   Vielleicht findest du eine Website, bei der detailliertere Informationen angegeben werden?

   Deine Ergebnisse:

4. Erläutere die Angaben in den Abbildungen mit der Übersicht über die Sicherheit der verwendeten Verschlüsselungsverfahren (vgl. Lerninhalte 1.8-04, S. 4-5).

   - „strong key exchange“:
   - „obsolete cipher“:

5. Öffne durch Klick auf das Schlosssymbol die Details zur Sicherheit der Adresse, die du in Aufgabe 3 angegeben hast. Bewerte die Sicherheit der Verbindung. Recherchiere auch in einer unabhängigen Quelle die aktuell als sicher eingestuften Protokollversionen und Verschlüsselungsverfahren.
   Gib den vollständigen Link und das Datum der Veröffentlichung an!

   Mögliche Suchbegriffe: „sichere verschlüsselungsverfahren“

   Sind die Ausführungen in den Lerninhalten 1.8-04, S. 4-5 noch aktuell?
   Beispielsweise ist zum Zeitpunkt der Erstellung dieses Arbeitsblattes nicht klar, wie lange SHA-2 noch als sicher gilt, weshalb bereits im Jahr 2012 SHA-3 standardisiert wurde (Stand: Januar 2017)

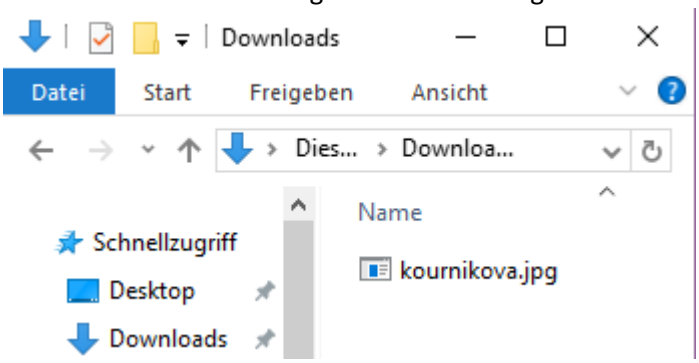
Dateiarchivierung

6. Wäge verschiedene Möglichkeiten zu Dateiarchivierung gegeneinander ab (Pro/Contra). Informiere dich auch im Internet über mögliche Software und Hardware für diesen Zweck. Plane das Vorgehen zum Erstellen eines Backups deiner Daten und setze dir einen Termin für die Umsetzung.

○ USB-Stick	Pro:	
	Contra:	
○ Externe Festplatte	Pro:	
	Contra:	
○ Optische Speichermedien	Pro:	
	Contra:	
○ Cloudspeicher	Pro:	
	Contra:	
Software		
○ Explorer bzw. Finder	Pro:	
	Contra:	
○ Dateiverwaltungs-werkzeuge	Pro:	
	Contra:	
○ Synchronisations-programme	Pro:	
	Contra:	
Planung	Beispiele: Preise; Tools; Internetdienste; Vorgehensweise; Termin	

Schadprogramme

7. Du erhältst scheinbar von einem Freund eine E-Mail. Den Dateianhang hast du heruntergeladen. Erläutere, um was für einen Dateityp es sich handelt, und äußere eine Vermutung, was in der Datei enthalten sein könnte. Eventuell kannst du auch im Internet nach ‚kournikova' suchen.
Hinweis: Die Dateinamenserweiterungen von ausführbaren Dateien sind unter Windows im Allgemeinen:
`.com`, `.exe`, `.bat`, `.cmd`, `.hta`, `.pif`, `.scf`, `.scr` oder `.vbs`.



Dateitp:

Vermutung zum Inhalt:

➢ Ergänze die Maßnahmen zum Überprüfen der Authentizität einer E-Mail.
(vgl. Modul 1.4 Risiken bei der Nutzung digitaler Kommunikationsformen)

- Abgleich
- Überprüfen
- Klären
- Internetrecherche mit Hilfe einer Suchmaschine nach einer prägnanten Formulierung, evtl. ergänzt um den Suchbegriff „spam". Begriffe in Grafiken sind nutzlos.

Schon die erste Maßnahme könnte dich hier misstrauisch machen:
Absenderadressen können gefälscht sein.

➢ Erläutere, wie sich Computerwürmer fortpflanzen. (vgl. Modul 1.4 Schadsoftware)

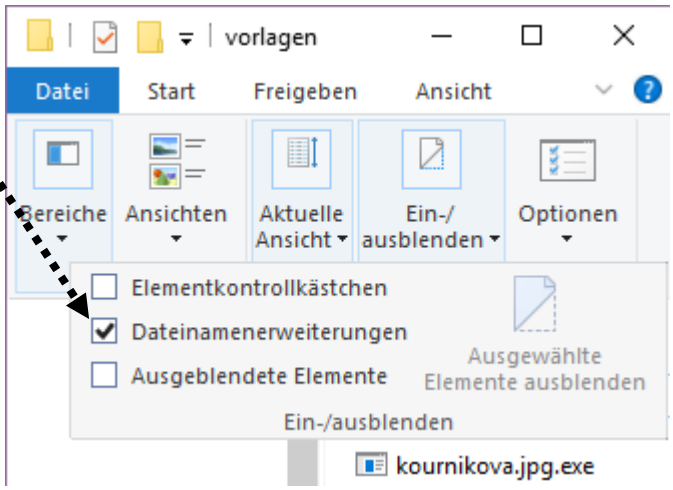
So kannst du ganz offizell eine E-Mail von einem guten Freund erhalten, die authentisch zu sein scheint. Sobald du den Dateianhang öffnest, wird das Schadprogramm aktiv.

Der Wurm kann dann eventuell auch weitere Sabotage- oder Spionagefunktionen ausführen.

➢ Äußere eine Vermutung oder suche im Internet nach der Information, worum es sich bei der E-Mail in Wirklichkeit handelt.

Dieser Wurm führte zum Glück für die Betroffenen keine weitere Schadfunktion aus. Dennoch wurde der Urheber zu 150 Stunden gemeinnütziger Arbeit oder alternativ zu 75 Tagen Gefängnis verurteilt.

8. Gib eine Maßnahme an, wie man sofort erkennen kann, um was für einen Dateityp es sich in Wirkklichkeit handelt.



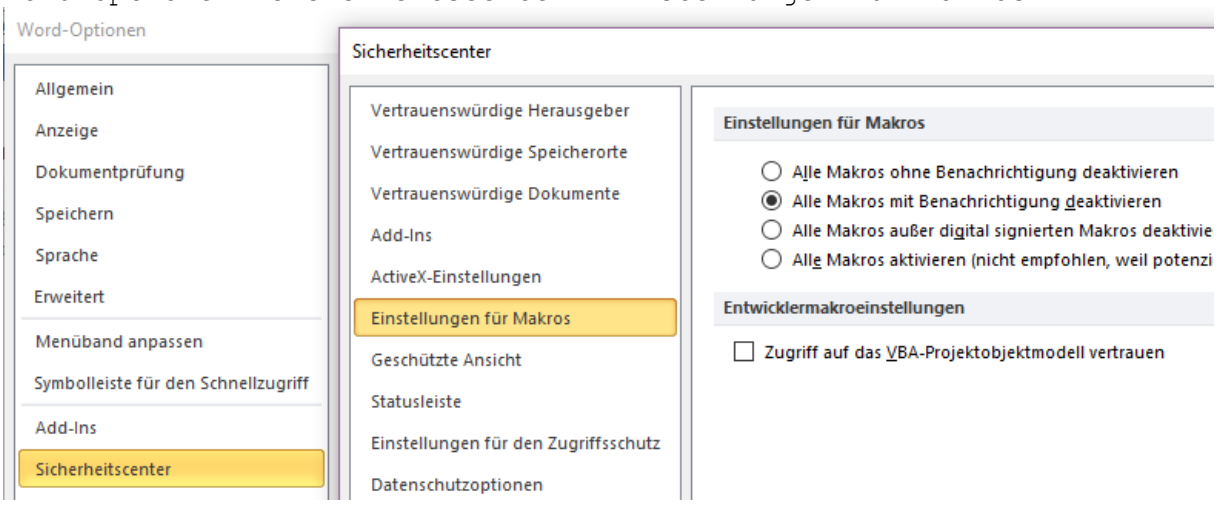
Hinweis:
Schadprogramme können nicht nur mit Hilfe ausführbarer Dateien eingeschleust werden. Durch Nutzung von Sicherheitslücken in Anwendungsprogrammen können auch über jpg-, doc- oder pdf-Dateien Schadprogramme eingeschleust werden.

9. Dateinamenserweiterungen für ausführbare Programme sind (vgl. Lerninhalte 1.8-02, S. 8): _____ – außerdem: .bat,.vbs, .scr,.wfs, .jse, .shs, .shb, .lnk oder .pif

➢ Bist du der Meinung, dass Dateinamenserweiterungen stören und man die Art der Datei an dem Icon zu der Datei erkennt?

- Viele ausführbare Dateiformate erlauben zusätzlich das Zuordnen von Icons zu einer Datei, so dass eine Datei wie „kournikova.jpg.exe“ nicht nur als „kournikova.jpg“ angezeigt wird, sondern auch noch das Icon einer Bilddatei erhalten kann und damit bei der Standardkonfiguration von Windows nicht von einer echten Bilddatei unterschieden werden kann.
- Aber auch innerhalb von vielen Anwendungsprogrammen kann Programmcode ausgeführt werden, so genannte Makros. Deshalb sollte das automatische Ausführen von Makros deaktiviert und von Dateien aus einer unbekannten Quelle auch nicht zugelassen werden.

Beispielsweise in Microsoft Word 2010 findet sich diese Einstellungen unter `Word-Optionen` -> `Sicherheitscenter` -> `Einstellungen für Makros`:



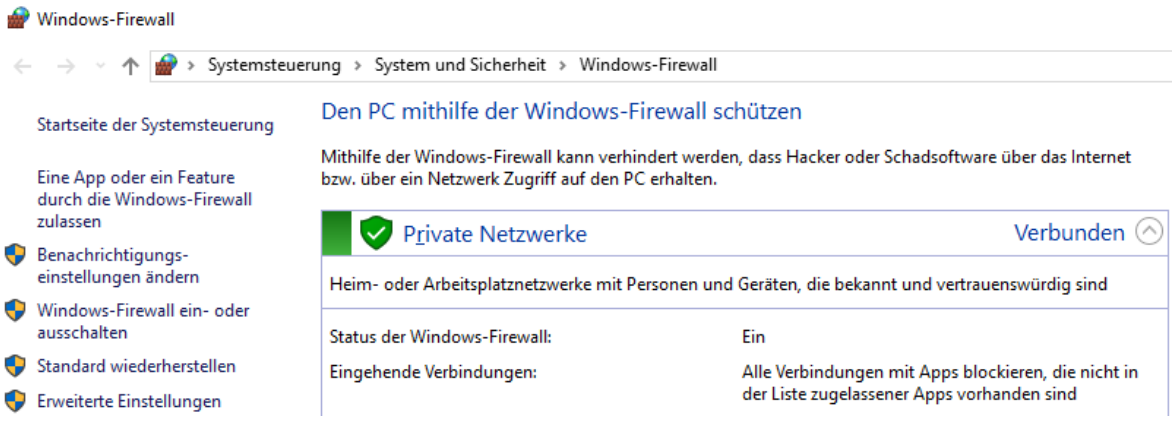
- Die Dateinamenserweiterung einer Datei, die ein Makro enthält, muss auch nicht beispielsweise `.doc` oder `.docx` lauten: Manche Anwendungsprogramme analysieren die Dateien und wenn eine .doc-Datei nachträglich in .rtf umbenannt wurde, führt Word das Makro dennoch aus.

10. Kontrolliere, ob das automatische Ausführen von Makros in dem Office-Programm, mit dem du meist arbeitest, deaktiviert ist.

Virenschutz

11. Nenne Sicherheitsmaßnahmen zu den Einfallstoren für Schadprogramme.

- Dateianhänge und Links in E-Mails
- Drive-by-downloads auf infizierten Websites
- Programme, die der Nutzer selbst installiert
- Direkte Angriffe auf Computer
  Hinweis: Eine **Firewall** blockiert Zugriffe auf das eigene Gerät.



- Makros