



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.

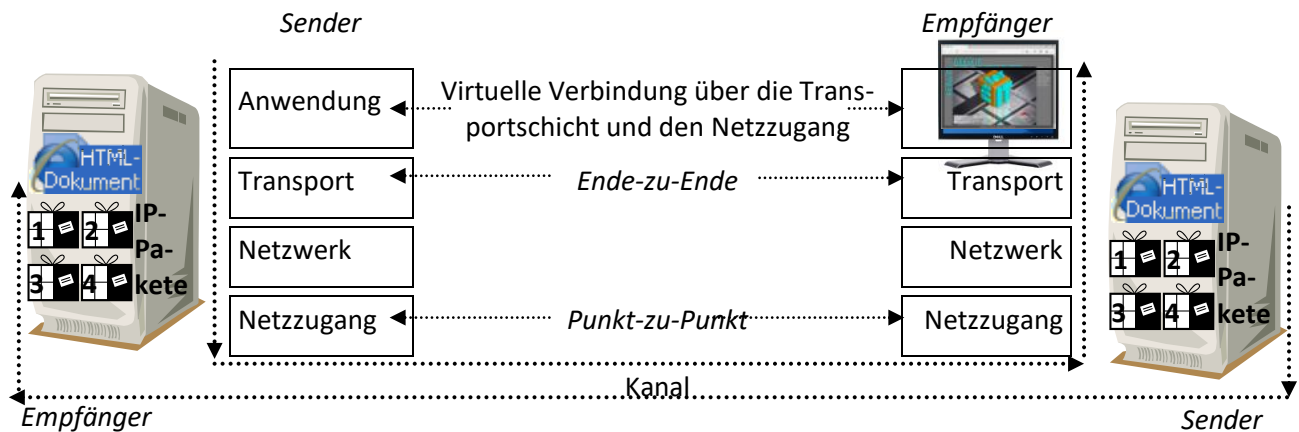
1. Was versteht man unter einem **Protokoll**? Nenne ein grundlegendes Protokoll zur Kommunikation im Internet.

*Unter einem **Protokoll** versteht man in der IT eine Sprache, mit der sich Computer in einem Netzwerk verständigen.*

Die meisten Dienste verwenden das TCP/IP-Protokoll.

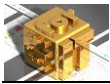
Ergänze:

- Ein **Host** ist ein Computer, der *Dienste in einem Netzwerk bereitstellt*.
 - Das Computerprogramm, das den Dienst anbietet, wird **Server** genannt, 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 Dienste nutzt*. Auch das Gerät, das Dienste nutzt, nennt man oft Client.
2. Ergänze: Der Sender zerlegt die Daten in **IP-Pakete** und übermittelt sie zum Empfänger.
IP ist die Abkürzung für Internet Protocol.



- Indem Nachrichten hin und her gesendet werden, tauschen die beiden Kommunikationspartner immer wieder die Rollen (Sender/Empfänger).
- Die eigentliche Kommunikation findet über die **Transportschicht** 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 **Anwendungsschicht** statt.
- Das grundlegende Protokoll zur Übermittlung von Webseiten auf der Anwendungsschicht ist **HTTP** (Hypertext Transfer Protocol).
- Bei **HTTPS** steht das **S** für **Secure**. 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).

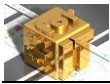
- „strong key exchange“: *Das Verschlüsselungsverfahren zum Austausch des Sitzungsschlüssels, der für die eigentliche Kommunikation verwendet wird, ist sicher.*
- „obsolete cipher“: *Das Verschlüsselungsverfahren für den Sitzungsschlüssel ist veraltet, also nicht mehr sicher – insbesondere der Algorithmus zur Überprüfung der Integrität (Vollständigkeit und Echtheit einer Nachricht).*

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.

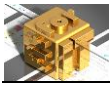
- USB-Stick
Pro: *preiswert; einfache Handhabung*
Contra: *kann leicht verloren gehen*
bei billigen Sticks oft minderwertiger Flash-Speicher
- Externe Festplatte
Pro: *hohe Speicherkapazität; einfache Handhabung*
Contra: *mechanisch anfällig; Daten durch natürliche Alterung*
nicht so lange haltbar wie bei anderen Medien
- Optische Speichermedien
Pro: *sehr günstig; lange haltbar*
Contra: *mechanisch anfällig (Kratzer)*
geringe Speicherkapazität
- Cloudspeicher
Pro: *theoretisch unbegrenzte Lebensdauer*
keine mechanische Zerstörung möglich
(z. B. bei Wohnungsbrand)
Contra: *Angriffe von außen; der Anbieter kann den Dienst einstellen*
bei (empfehlenswerten) Bezahldiensten laufende Kosten

Software

- Explorer bzw. Finder
Pro: *kostenlos (Betriebssystem-Zubehör)*
Contra: *unkomfortabel: ersetzt beim Kopieren von Verzeichnisbäumen*
immer nur entweder keine oder alle Dateien
- Dateiverwaltungswerkzeuge
Pro: *komfortabler Abgleich ganzer Verzeichnisbäume*
es gibt auch Freeware und Shareware
Contra: *die Kopieraktion muss manuell ausgeführt werden*
- Synchronisationsprogramme
Pro: *zuvor festgelegte Aktionen werden automatisch ausgeführt*
Contra: *versehentlich gelöschte Dateien werden auch im Backup gelöscht*
→ auf eine Versionsverwaltung achten!

Planung

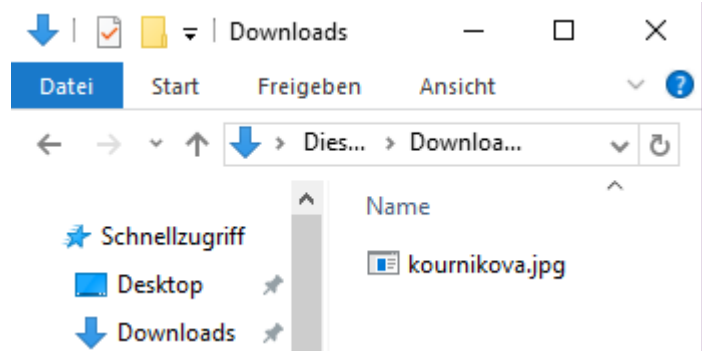
Beispiele: Preise; Tools; Internetdienste; Vorgehensweise; Termin



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.



Dateityp: Die Dateinamenserweiterung ist .jpg, also dürfte es sich um eine Bitmapgrafik handeln.

Vermutung zum Inhalt: Es wird wohl ein Bild der ehemaligen russischen Tennisspielerin Anna Kurnikowa (französische Schreibweise: Anna Kournikova) enthalten sein.

- Ergänze die Maßnahmen zum Überprüfen der Authentizität einer E-Mail. (vgl. Modul 1.4 Risiken bei der Nutzung digitaler Kommunikationsformen)
 - Abgleich der Absenderadresse mit dem E-Mail-Text.
 - Überprüfen der Grammatik und Rechtschreibung.
 - Klären der Notwendigkeit einer persönlichen Anrede.
 - 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)

Würmer können die E-Mail-Adressen im System auslesen

und diese sowie sich selbst an alle Adressen senden.

So kannst du ganz offiziell 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.

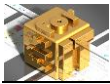
- Äußere eine Vermutung oder suche im Internet nach der Information, worum es sich bei der E-Mail in Wirklichkeit handelt.

Eine Suche nach „kournikova wurm“ führt zu der Information,

dass es sich um einen Wurm handelte, der sich im Jahr 2001

mit Hilfe des Outlook-Adressbuchs als Massenmail versendete.

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.



1.8 Grundlagen elektronischer Datenverarbeitung

Arbeitsblatt 13 Maßnahmen zur Datensicherheit

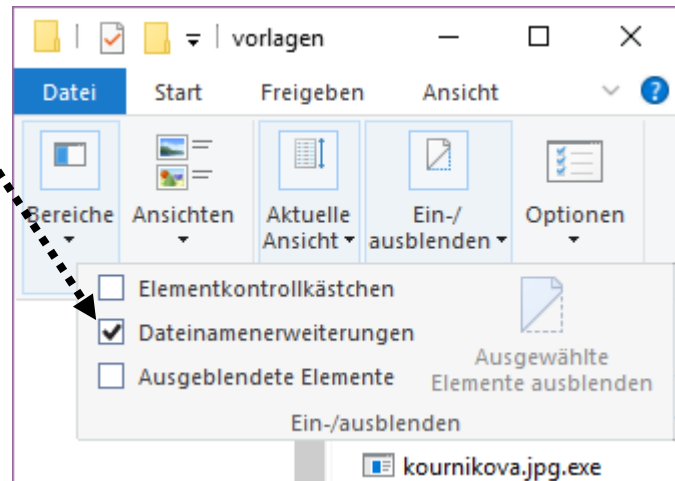
Lösungen

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

Aktivieren der Dateinamenerweiterungen im Windows Explorer.

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.



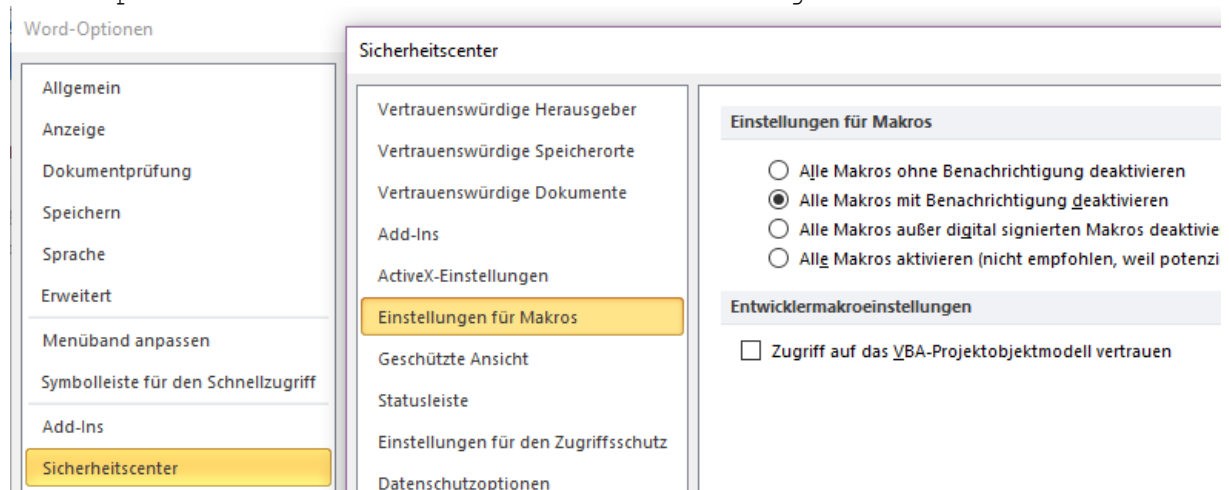
9. Dateinamenerweiterungen für ausführbare Programme sind (vgl. Lerninhalte 1.8-02, S. 8):

.exe, .com, .cmd – außerdem: .bat, .vbs, .scr, .wfs, .jse, .shs, .shb, .lnk oder .pif

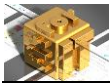
- Bist du der Meinung, dass Dateinamenerweiterungen stören und man die Art der Datei an dem Icon zu der Datei erkennt?
- Viele ausführbare Dateiformate erlauben zusätzlich das Zuordnen von Icons zu einer Datei, so dass eine Datei wie „kournikova.jpg.exe“ nicht nur als „kournikova.jpg“ angezeigt wird, 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 Dateinamenerweiterung 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

Keine Dateien aus unbekannten Quellen öffnen.

Keinen zweifelhaften Links folgen;

im Zweifelsfall lieber den angeblichen Absender kontaktieren.

- Drive-by-downloads auf infizierten Websites

Fragwürdige Angebote meiden.

(z. B. Tauschbörsen; Lockangebote mit geknackter Software oder Musik;

Server, auf denen Hackerwerkzeuge heruntergeladen werden können)

Immer aktuelle Versionen von Virenschutzprogramm,

Browser und Plugins (z. B. Java, Adobe Reader und Flash)

verwenden (automatische Updates!).

- Programme, die der Nutzer selbst installiert

Auf die Seriosität der Downloadserver achten;

Herausgeber und Software auch in unabhängigen Quellen prüfen

- Direkte Angriffe auf Computer

Hinweis: Eine **Firewall** blockiert Zugriffe auf das eigene Gerät.

 Windows-Firewall



Firewall auf dem Gerät und dem WLAN-Router aktivieren bzw. aktiviert lassen!

Freigaben für die Firewall („Zugriff erlauben“) nur wohl überlegt erteilen

und sofort wieder löschen, wenn sie nicht mehr benötigt werden.

- Makros

Automatische Ausführung von Makros in Anwendungsprogrammen deaktivieren