Grundlagen

Die Basis einer jeden Sicherheitsstrategie ist das auch technische Verständnis der Vorgänge rund um Hard- und Software. Sich ein solches - Schritt für Schritt - anzueignen, Wissen zu erwerben und Kompetenzen zu entwickeln, ist demnach die langfristig beste Schutzstrategie.

Diese Aussage mag nicht jedermann/frau gefallen - Lebenszeit ist eine beschränkte Ressource - aber die Forderung lautet ja auch nicht, ein Ingenieursstudium zu machen. Dazu kommt: Wir sind eine Schule - also warum nicht Lernen als Strategie einsetzen?

Ein paar Beispiele und Prinzipien, die in den folgenden Wochen und Monaten hier im Wiki weiter ausgearbeitet werden.

Die Basics

Die folgenden Regeln gelten immer, stellen die absolute Grundlage dar, ohne die keine weiteren Schritte irgend einen Sinn machen:

- Arbeite nicht mit **Administrator**-Rechten, sondern lege Dir für die täglichen Aufgaben und Arbeiten ein Konto mit eingeschränkten Rechten an. HowTo
- Sichere Dein **Benutzerkonto** durch ein Passwort. Boote nicht in Dein Profil, sondern zum Login-Screen. Lege für jeden Benutzer ein eigenes Konto auf dem von mehreren Personen genutzten Rechner an. Melde Dich ab, wenn Du Deinen Rechner nicht verwendest. Stelle Deinen Bildschirmschoner so ein, dass dieser mit einem Kennwort entsperrt werden muss.
- Schütze Deine **Passwörter**. Wähle komplexe Passwörter - hier steht, wie das geht.
- Gib in fremden Netzen (z.B. Internetcafe) und auf unverschlüsselten Internetverbindungen nach Möglichkeit keine Passwörter ein. Oder nutze für derartige Seiten und Fälle zumindest nicht ein Passwort, das Dir etwas Wert ist. Lege Dir für unverschlüsselte Seiten besondere Passwörter an bzw. nutze für den Urlaub E-Mail Accounts bei Freemailern, die Du hinterher löschst. Arbeite in der Urlaubszeit mit Umleitungen.
- Installiere Dir unter Windows auf jeden Fall einen **Virenscanner** und sorge in dessen Programmeinstellungen dafür, dass dieser sich täglich mehrfach aktualisiert.
- Aktiviere unter Windows die **Firewall** im Sicherheitscenter. HowTo
- Halte Deine **Software** immer aktuell. Vor allem: Betriebssystem, Java, Browser, Mail-Client, PDF-Reader und Dein Office. Wenn Dein Betriebssystem und Deine Programme keine Auto-Update- oder Update-Warn-Funktionalitäten mitbringen, dann verzichte komplett darauf [1)]. HowTo
- Verzichte auf die Installation von Software aus unbekannten Quellen - nutze Dienste und Prüfroutinen vertrauenswürdiger Anbieter wie Heise: http://www.heise.de/download/
- Konfiguriere die von Dir genutzten Programme in Hinblick auf Deine Sicherheit. Wie dies für Deinen Browser funktionieren kann, steht z.B. auf den folgenden Seiten: Internetsicherheit.
- Halte Deinen Rechner sauber: Wenn du Software nur mal angucken oder testen willst, aber evtl. nicht wirklich brauchst, dann nutze hierfür nicht Dein Arbeitsgerät, sondern einen anderen Rechner oder noch besser gleich eine virtuelle Maschine. Hier steht, wie das geht: http://lehrerfortbildung-bw.de/netz/virtual/

Hilfreiches

Die folgenden Schritte, Prinzipien und Hinweise solltest Du beherzigen, da sie Dir die Verwaltung Deiner Sicherheitskonzepte und -einstellungen erleichtern:

- Wenn eine **Internetseite** auch verschlüsselt über HTTPS angeboten wird, dann nutze ausschließlich die HTTPS Seiten.
- Lass Deine **Mails** nicht auf dem Server Deines Providers oder in der Cloud liegen, sondern hole Dir diese über eine verschlüsselte Verbindung (POP3s, IMAPs) auf Deinen eigenen Rechner.
- Trenne Programm und Betriebssystem von Deinen **Daten**. Nur dann ist ein Backup Deiner Daten einfach möglich. Sprich nicht nur über Backups - erstelle diese auch regelmäßig und lagere diese nach Möglichkeit nicht nur zu Hause (Wohnungsbrand!).
- Verwende keine **Backup**-Programme, die proprietäre Formate nutzen [2)] und Dich somit an einen bestimmten Hersteller fesseln, sondern Funktionen, die dafür sorgen, dass Deine Daten - so wie diese sind - regelmäßig auf eine externe Platte / in die Cloud geschrieben werden. Wirf als Linux Nutzer einen Blick auf BackinTime, als Apple-Nutzer einen Blick auf Time Machine und als Windows-Nutzer auf dieses Script.
- Nutze keine **Verschlüsselungssoftware**, die nicht OpenSource ist: Niemand kann überprüfen, was diese wirklich tut. Verschlüssele Deine sensiblen Daten mit Hilfe von TrueCrypt.
- Verschlüssele Deine E-Mails, wenn diese sensible Informationen beinhalten: HowTo
- Wenn Dein Gegenüber keine verschlüsselten E-Mails empfangen oder versenden kann, dann sprich telefonisch - oder besser noch: in real life - ein Kennwort ab. Verschicke dann per Mail einen mit diesem Kennwort verschlüsselten TrueCrypt-Container oder notfalls auch ein verschlüsseltes 7ZIP Archiv [3)].
- Verwende keine **Cloud**-Dienstleister für sensible Daten, deren Server nicht in Europa stehen (z.B. DropBox oder die Apple- und MS-Cloud). Die Datenschutzbestimmungen in den USA sind ein Witz. Nutze regionale Alternativen wie z.B. HiDrive oder noch besser: OwnCloud auf Deinem eigenen Server [4)].
- Nutze **soziale Netzwerke** mit Bedacht. Lies Dir die Hinweise auf der Seite Soziale Netze durch.
- Informiere Dich über die aktuelle Bedrohungslage im Internet. Idealerweise durch das Abo eines Feeds eines bekannten Dienstleisters wie Heise. Siehe hierzu die entsprechende Seite im Wiki: Bedrohungslage

Weiter: Internet

1)
Dazu zählt auch fast jedes Programm aus den sog. Schulbuchverlagen, die von CD installiert werden. Schon bei der Auslieferung sind diese meist völlig veraltet.
2)
Proprietäre Formate: Manche Backup-Programme schreiben Deine Daten in Container, die nur das Backup-Programm, das diesen Container angelegt hat, auch wieder auslesen kann.
3)
ZIP bietet ebenfalls eine Verschlüsselung an, diese ist aber leicht zu knacken. Du musst demnach unbedingt das Dateiformat 7z für den sicheren Austausch von Informationen und Daten nutzen!
4)
Der Test von OwnCloud für das KvFG Netz ist zu Beginn des Jahres 2012 angelaufen.