Stand 31.01.2020

M. Diener/Version für Institutsmitglieder

Sicherheit im Inter- und Intranet und Datensicherheit

Unbedingt zu beachten sind generell folgende grundlegenden Sicherheitsmaßnahmen:

1. Windows-Updates sofort bei Erscheinen installieren.
2. Antiviren-Programm benutzen und aktuell halten.
3. Sicheren Web-Browser verwenden (auch SicherheitsAddons aktuell halten).
4. Sicheres Email-Programm verwenden (sichere Anzeige- und Sendeeinstellung wählen).
5. Sichere Einstellung des Betriebssystems.
6. Nie Rechner mit veralteten Betriebssystemen (veraltet sind: Windows 2000, XP, Windows Vista, Windows 7) an das Netzwerk anschließen oder gar ins Internet gehen!
7. Nie mit Administratorrechten in Internet gehen.
8. Regelmäßig Backups wichtiger Daten erstellen.
9. Generelle Vorsichtsmaßnahmen („gesunder Menschenverstand“).

Verhaltenscode:

Kompletten Schutz gibt es nicht! Daher:

- Gesundes Misstrauen gegenüber fremden oder merkwürdig formulierten Emails, auch von anscheinend bekannten Personen.
- Im Zweifelsfall Quelltext einer Email anschauen (Thunderbird: `/Ansicht/Nachrichtenquelltext`).
- Nie direkt Makros aktivieren bei Office-Dateien (Word, Excel), die direkt aus dem Netz geladen wurden!
- Für verschiedene Vorgänge unterschiedliche Passwörter verwenden! (ggf. Passwort-Manager wie etwa Keepass (http://sourceforge.net/projects/keepass/) benutzen).
- Betriebssystem und Virenschutzprogramm immer aktuell halten.

Falls doch Befall durch einen Virus oder Trojaner:

- PC sofort vom Netz nehmen. Am besten ausschalten, so dass man versuchen kann durch Booten mit einem anderen Betriebssystem (Linux) noch Daten zu retten.

1. Windows-Updates

Bei Windows 10 werden Updates normalerweise automatisch installiert. Trotzdem empfiehlt es sich, über `PC-Einstellungen/Update und Sicherheit/Windows updates` Updates suchen zu lassen, um sicher zu gehen, dass wirklich alle Updates installiert worden sind.
Die manuelle Suche nach Updates befindet sich bei Windows 8 unter `Systemsteuerung/Windows Update`


Dieses Zeichen in der Task-Leiste zeigt, dass keine Sicherheitsprobleme von Windows erkannt worden sind.


Dieses Zeichen in der Task-Leiste von Windows 10 zeigt an, dass ein Neustart zum Abschluss eines Updates notwendig ist.

2. Antiviren-Programm

Sophos Endpoint vom HRZ muss installiert sein, wenn ein PC an eine Netzwerksteckdose angeschlossen ist.
Ab und zu prüfen (Startseite von `Sophos Endpoint/Informationen` (unten rechts)), ob die Aktualisierungen regelmäßig erfolgen.


Dieses Zeichen in der Task-Leiste zeigt, dass Sophos Endpoint läuft.

Cave: Sophos Endpoint blockiert ihm unbekannte Geräte, die an den PC angeschlossen sind (das kann bis zu Dongles von lizenzierter Software oder Kameras gehen). Falls Geräte nicht funktionieren, in Sophos den Schalter „Gesteuerte Elemente“ anklicken zur Kontrolle, ob ggf. ein Gerät von Sophos blockiert wurde. Das Gerät muss dann dem Rechenzentrum (support@hrz.uni-giessen) oder dem dort zuständigen Mitarbeiter (markus.kopitzara@hrz.uni-giessen.de) mitgeteilt werden, damit seine Freischaltung bei Sophos Central beantragt wird.

Cave: Sophos Endpoint kontrolliert das Surf-Verhalten im Internet. Wenn Seiten mit Inhalt betreten werden, die Sophos als verdächtig (bis „unkoscher“) klassifiziert, wird der Rechner isoliert (alle Netzverbindungen unterbrochen).

3. Web-Browser

Wo immer möglich, Mozilla **Firefox** (Quelle: http://www.mozilla.com/) als Browser verwenden.
Ganz wichtig: Regelmäßig Updates der Browser installieren! Updatesuche kann manuell mit dem Menüpunkt `/Hilfe/Über Mozilla Firefox` gestartet werden.

Auch die Add-Ons (Plug-Ins) regelmäßig auf Aktualität prüfen.
Das geht unter Firefox mit dem Menüpunkt `/Extras/Add-Ons` → Überprüfen Sie, ob Ihre Plugins aktuell sind

Optional können z.B. folgende sicherheitserhöhende Add-Ons (→ Erweiterungen) installiert werden:

- BetterPrivacy (gegen Local shared objects, also sog. Flash Cookies)
- uBlock Origin (blockiert Werbung und Tracker)
- Ghostery (blockiert Werbung und Tracker)
- FlashBlock (verhindert automatisches Starten von Flash Videos aus einer Seite, welche direkt beim Öffnen einer Seite Schadsoftware übertragen können)

Vermeiden: Internet Explorer (Active-X-Steuerelemente können missbraucht werden; dazu reicht schon der Besuch einer entsprechend präparierten Webseite).
Gute Alternative: Edge als Virtual Machine für erfahrene Nutzer.

4. Email

Emails öffnen mit:
Mozilla **Thunderbird** (Quelle: http://www.mozilla-europe.org/de/;
persönliche Einstellungen am besten konfigurieren über:
http://www.uni-giessen.de/fbz/svc/hrz/svc/komm/email/conf)
Auf Aktualisierungen von Thunderbird achten und diese regelmäßig durchführen!

Die Anzeige von html-Emails und das Ausführen von Skripten sollten generell in Mailprogrammen ausgeschaltet werden, da bei diesen Mailclient-Einstellungen schon Emails ohne Attachment den Rechner zerstören können. Daher als Sicherheit gegen HTML-Schadcode bzw. gegen Links, die „verkappt“ in einem Emailtext angezeigt werden:
`/Ansicht/Nachrichteninhalt/Reiner Text`

`/Extras/Konteneinstellungen/Verfassen&Adressieren:`
Bei allen Email-Konten Haken wegnehmen bei „Nachrichten im HTML-Format verfassen“.

Riskant: Outlook (Active-X-Steuerelemente können durch Viren verwendet werden, üblicherweise keine Ansicht der echten Absenderadresse einer Email).

Anhänge und Links in Emails:
Keine unbekannte Links anklicken und keine unbekannten Anhänge öffnen! Immer kontrollieren, ob Absendername und echte Absender-Email-Adresse kongruent sind.

Beim Öffnen von pdf- oder Worddateien können Skripte (Makros) Viren oder Trojaner einschleusen,
Daher:

- Unbekannte pdfs am besten mit einem pdf-Reader öffnen, der keine Skripte erlaubt (z.B. Sumatra PDF; Quelle: https://www.sumatrapdfreader.org/free-pdf-reader.html).
- Word-Einstellungen: Datei/Optionen/Sicherheitscenter/Einstellungen für Sicherheitscenter: Alle Makros deaktivieren.
  Das gleiche gilt auch für alle anderen Anwendungen aus Microsoft Office (wie z.B. Excel oder Powerpoint).

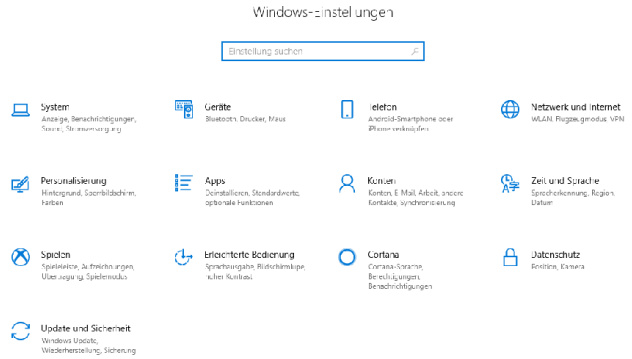
Um das Ausspähen durch Trojaner wie Emotet zu reduzieren (etwa in Outlook-Kalendern von Personen, mit denen man kommuniziert), Listen (von mehr als 2 Empfängern) immer als Blindkopie (BCC, Blind copy) versenden, damit keine Beziehungsnetzwerke für das Fälschen von Emails aufgebaut werden können.

Neue Sicherheitsrichtlinien (01-2020) des HRZ:

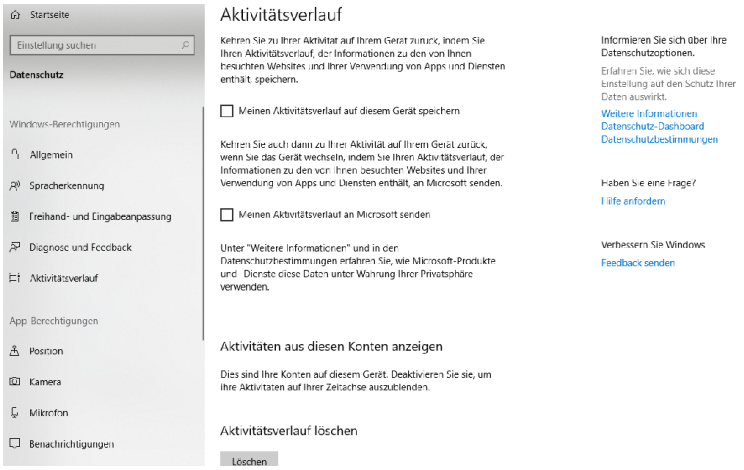
- Anhänge, die Makros enthalten, kommen in Quarantäne (?)
- Anhänge mit alten Office-Formaten (z.B. doc) werden zurückgewiesen.
- Emails mit Absendernamen *@uni-giessen.de, die nicht vom Mailserver der Universität versandt wurden, werden blockiert (→ besserer Schutz vor gekaperten Uni-Emailadressen).

5. Datenschutz- und Sicherheitseinstellungen für Benutzer von Windows 10

Bei „Datenschutz“ (`Einstellungen/PC-Einstellungen/Datenschutz`) alle Zugriffe (Liste auf der linken Seite durchklicken) mit Ausnahme von ggf. Skype abschalten. Ansonsten werden Daten unkontrolliert an Microsoft gesendet.



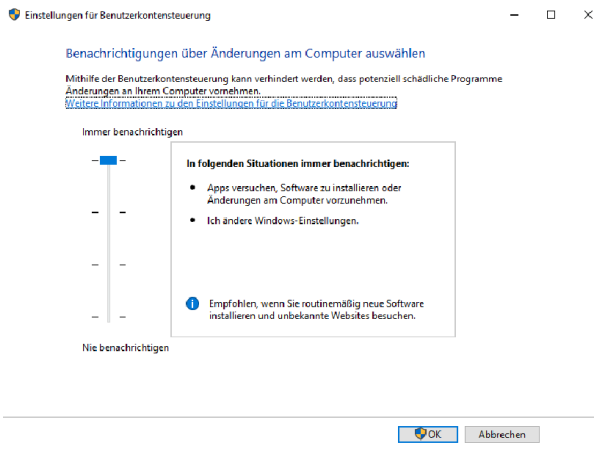
Hier den Schalter Datenschutz auswählen.



Hier auf der linken Seite (Windows-Berechtigungen) alle Parameter durchgehen und auf „Nein“ stellen.

Diese Einstellung sollte von Zeit zu Zeit überprüft werden, da sie bei Windows-Updates (z.B. von Skype) verändert werden können!
Ggf. Ausnahme: Kamerazugriff, Mikrofonzugriff und Hintergrundaktivität für Skype erlauben.

Einstellung für Benutzerkontensteuerung
`Systemsteuerung/Benutzerkonten/Einstellungen der Benutzerkonten ändern` → `Benachrichtigungen über Änderungen am Computer` auswählen (Direktzugriff: Befehlsfeld): `UAC` eingeben [UAC = user account control]
Schieberegler auf ganz oben (immer benachrichtigen) einstellen



Einstellung für Benutzerkontensteuerung.

Am besten auch das automatische Öffnen/Abspielen von DVDs oder Datensticks unterbinden mit:
`/Einstellungen/Geräte/Automatische Wiedergabe: Aus`

6. Rezente Windowsversionen verwenden

Nur mit Windows-Versionen ins Netz gehen, die von Microsoft noch mit Sicherheits-Updates versehen werden. Das sind Windows 8.1 und Windows 10.

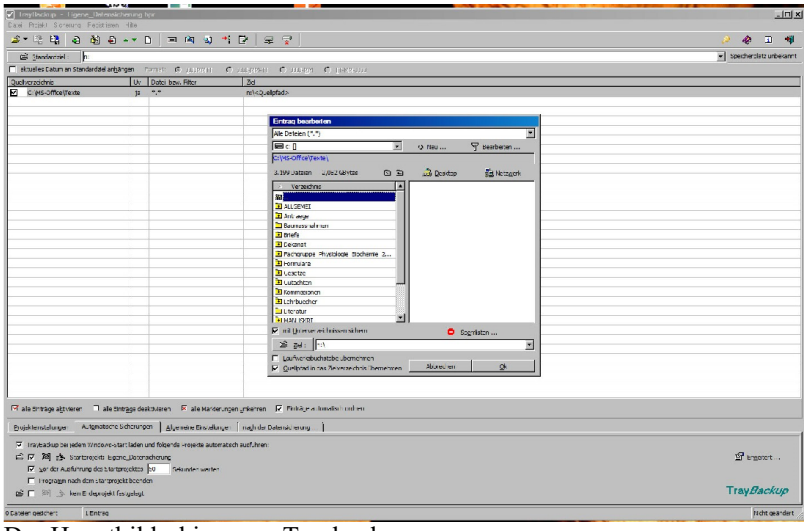
Rechner mit älteren Windows-Versionen, die z.B. zum Betreiben von bestimmten Geräten benötigt werden, dürfen nicht ans Netz. Es darf auch kein Netzstecker eingesteckt sein!

7. Benutzerrechte

Das Surfen im Netz oder das Öffnen von Emails sind wesentlich ungefährlicher, wenn kein Administrator-Account dazu verwendet wird.
Daher immer nur mit „normalen“ Benutzerrechten ins Netz gehen und Administratorrechte nur transient benutzen (z.B. durch `Als Administrator ausführen`) mit einem separaten Administratorkonto.

8. Backups

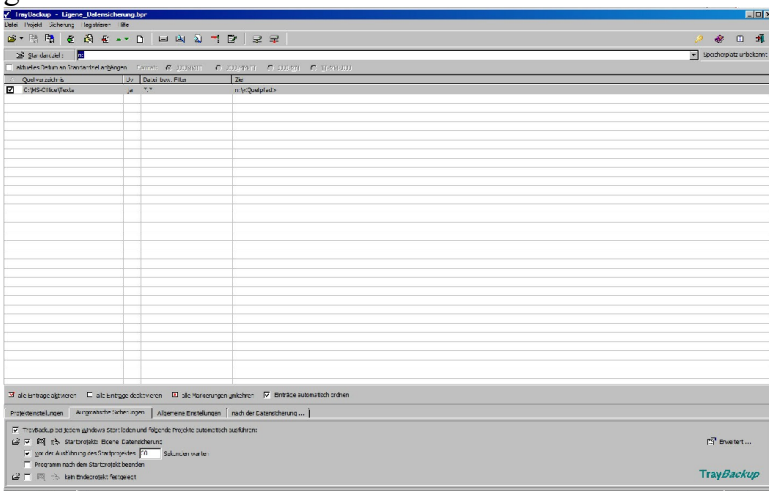
Regelmäßig Backups machen z.B. mit **Traybackup** (Quelle: http://www.traybackup.de/). Dort Quellverzeichnisse und Ziel (externe Festplatte) einstellen. Programm so einstellen, dass das jeweilige Speicherprojekt beim Hochfahren von Windows automatisch gestartet wird.



Der Hauptbildschirm von Traybackup.

In den entsprechenden Spalten (Quellverzeichnis und Ziel) die Verzeichnisse, ob mit oder ohne Unterverzeichnisse (UV) oder Datei/Filter (z.B. *.docx) auswählen. Dann das Projekt speichern, z.B. als „Eigene_Sicherung“

Im Reiter automatische Sicherungen einstellen, dass das Projekt bei jedem Windows-Start gestartet wird.



Der Bildschirm zum Einstellen der automatischen Backups.

Externe Platten nach dem Backup ausschalten (damit sie nicht warm laufen oder von Verschlüsselungstrojanern befallen werden können).

9. Generelle Vorsichtsmaßnahmen

- Bei Mails von Unbekannten oder merkwürdig formulieren Mails von scheinbar bekannten Absendern keine Anhänge öffnen und keine Links anklicken. Im Zweifelsfall Quelltext der Email anschauen (Thunderbird: `/Ansicht/Nachrichtenquelltext`).
- Keine Makros/Skripten erlauben von Office-Dateien (Word, Powerpoint, Excel), die aus Email-Anhängen stammen.
- Software nur von vertrauenswürdigen Quellen herunterladen.
- Kein Surfen in ungeschützten Netzen zu Seiten, die nicht verschlüsselte Kommunikation haben (also nur „`http://`“ statt „`https://`“ in der Adressleiste anzeigen). Am sichersten ist die Verwendung von VPN.