Sicherheit für Anwender

– Checkliste –

- **Einsatz eines Virenscanners**, der regelmäßig mit neuen Virenkennungen auf den neuesten Stand gebracht wird (besser: permanente automatische Aktualisierung) zur Abwehr von Viren, Würmern und Trojanern

- **Ein generell umsichtiges und wachsames Verhalten im Umgang mit E-Mail-Anlagen** zur Abwehr von Viren, Würmern und Trojanern
  - E-Mail Anhänge nur durch Doppelklick öffnen, wenn sicher ist, dass der Anhang keine Viren enthält
  - Dateinamenerweiterungen einblenden
  - Anhänge nicht automatisch öffnen
  - Vorsicht bei Office-Dokumenten als E-Mail-Anhang

- **Einsatz der jeweils neuesten Web-Browser mit sicherer Konfiguration und mit den aktuellsten Sicherheits-Korrekturen,** denn aktive Elemente und Softwarefehler bieten Schlupflöcher für Eindringlinge und Viren

- **Ein generell umsichtiges und wachsames Verhalten im Umgang mit dem Internet** zur Abwehr von Viren und Trojanern
  - Downloads nur durchführen, wenn die Website absolut vertrauenswürdig ist

- **HTML-Mail vermeiden** zur Abwehr von Viren, Würmern und Trojanern

- **Sorgfältiger Umgang mit Passwörtern,** denn Missbrauch ermöglicht vollen Zugriff

- **Regelmäßiges Einfahren von Sicherheits-Korrekturen (Patches) für die Betriebssysteme,** denn Betriebssystemfehler bieten Schlupflöcher für Eindringlinge und Viren

- **Was nicht benötigt wird, sollte deinstalliert oder zumindest deaktiviert werden,** denn offene Ports sind offene Türen für Angreifer und Viren

- **Keine Datei- und Drucker-Freigaben**, solange eine Verbindung mit dem Internet besteht, denn offene Standard-Ports sind offene Scheunentore für Eindringlinge und Viren