Wie kann ich Outlook Express (viren-)sicher einstellen und betreiben?

Grundsätzlich gilt, neben der Empfehlung stets die aktuellsten Versionen und danach erscheinende Sicherheitsfixes umgehend zu installieren: Öffne niemals (!) Attachments (= Dateianhänge) von einem Absender, den Du nicht kennst. Da sich aber einige der "Schädlinge" der Einträge des Adressbuchs bedienen, um sich zu verbreiten, müssen weitere Vorsichtsmaßnahmen gelten. So sollte der Absender das Attachment z.B. in seinem Text erwähnt haben. Im Zweifelsfall, oder wenn man unverlangt eine Datei zugeschickt bekommt, sollte man immer rückfragen, um sicher zu gehen. Wenn einem ein Deutschsprechender User plötzlich eine englische Mail mit Attachment schickt, sollten ebenso alle Alarmglocken schellen. Sobald ein Attachment oder HTML im Spiel ist, ist Skepsis angesagt. Wenn man ein Attachment erhalten hat, das soweit "völlig ok" ist, sollte man trotzdem überprüfen, ob nicht doch ein Virus mit dabei ist. D.h. die Datei vor dem Öffnen grundsätzlich zuerst auf die Festplatte speichern. Dann mit einem Virenscanner (aktuelle Virus-Definitionsdateien!) auf Viren überprüfen und anschließend ggf. öffnen.

Für die (Sicherheits-)Einstellungen gilt:

In OE selbst muss unter Extras | Optionen | Sicherheit die Zone für eingeschränkte Sites eingestellt sein. Da sich OE mit dem IE die Sicherheitsoptionen (teilweise, je nach Einstellung) teilt, sind im IE noch ein paar Einstellungen nötig: Extras | Internetoptionen | Sicherheit. Hier markiert man die Zone für eingeschränkte Sites (!) und klickt auf Stufe anpassen. In den dortigen Einstellungen sollte man alles deaktivieren, das einem verdächtig erscheint (wenn es nicht bereits deaktiviert ist...). Dazu muss insbesondere Active Scripting (Java Script) und ActiveX zählen. Optimalerweise sollte alles deaktiviert oder auf Eingabeaufforderung stehen, es sollte nichts ohne Rückfrage automatisch ausführbar (= "aktiviert") sein.

Ab IE/OE 6 SP1 gibt es außerdem noch eine neue Option unter Extras | Optionen | Lesen: Diese erlaubt es einem, alle Nachrichten, egal ob HTML oder Text, als reinen Text zu betrachten. Aus Sicherheitsgründen sollte man diese Option auf jeden Fall aktivieren (by default ist sie es nämlich leider (noch?) nicht). So wird ein optimaler Schutz vor Viren, Würmern und anderen Schädlingen ebenso erreicht, wie verhindert wird, dass Emails Browserfenster öffnen oder Spam "nach Hause telefoniert" (= Überprüfung der vollgemüllten Adresse durch das Nachladen von Pseudobildern, etc.). Der HTML-Teil der Nachricht erscheint, ebenso wie evtl. angehängte Dateien, als Attachment (Büroklammer-Symbol). Beim Öffnen der Attachments gelten natürlich die inzwischen bekannten Sicherheitsregeln. Leider wurde für diese Option kein Button für die Symbolleiste hinzugefügt, über den man leicht zwischen "HTML an" und "HTML aus" umschalten könnte.

Wer übervorsichtig ist, kann auch noch die automatische Vorschau von Nachrichten deaktivieren: Ansicht | Layout | [_] Vorschau. Das sollte, mit obigen Sicherheitseinstellungen - insb. der PlainText-Option - aber nicht nötig sein. Es muss allerdings angemerkt werden, dass es tatsächlich Schädlinge gibt, bei denen es genügte, die Nachrichten im Vorschaufenster zu betrachten (Klez...), falls man nicht entsprechend auf dem aktuellen Stand ist oder sein OE wie hier aufgeführt eingestellt hat (auffallend ist, dass sich alle Schädlinge HTMLs bedienen, mit der Deaktivierung von HTML ist man daher auf der sichereren Seite): Es sollte daneben

selbstverständlich sein, dass man die aktuellsten Sicherheitspatches stets umgehend installiert und sich informiert, welche Schädlinge im Moment die Runde machen.

Hilfreich ist auch, wenn bei allen Dateitypen die Rückfrage, ob geöffnet oder gespeichert werden soll, aktiviert bleibt. Diese lässt sich im Windows-Explorer ggf. wieder aktivieren: Ansicht (oder Extras) | (Ordner-)Optionen | Datei-Typen => entspr. Dateityp (z.B. *.zip) suchen | Eigenschaften | [x] Öffnen nach dem Download bestätigen.

Für diejenigen, die OE6SP1 (noch) nicht installiert haben oder es nicht dürfen/können und HTML dadurch nicht abschalten können: Durch obige Einstellungen kann man zwar "schädliches HTML" weitgehend abmildern, aber gegen normales HTML, das OE nativ unterstützt, kann man so nichts machen. Was das heißen soll? Mit "normalem HTML" kann eine HTML-Email z.B. ein Browserfenster öffnen um dort etwas zu laden oder die (Spam-)Email lädt Bilder, etc. aus dem Internet nach und teilt ihrem Server auf diesem Wege manchmal gleichzeitig auch noch mit, dass die Adresse, an die die Email geschickt wurde, tatsächlich existiert und gelesen wird (praktisch ein Garant für mehr Spam...). Dies kann man dadurch verhindern, dass man offline arbeitet (Datei | Offlinebetrieb, Doppelklick auf das Monitor-Symbol in der Statusleiste oder den passenden Button dafür in die Symbolleiste über (Rechtsklick | Anpassen) legen).

Sollte man sich dennoch einen Virus eingefangen haben, gilt: Rechner abschalten und nichts mehr damit machen. Mit einem anderen Rechner ggf. die aktuellste Anti-Viren-Software besorgen und dann versuchen den anderen Rechner vom Virus zu reinigen. Dies kann, je nach Viren-Scanner, unter DOS geschehen. Über eine Bootdisk kann man auch versuchen, wichtige Daten zu sichern (Vorsicht! Diese können ebenfalls vom Virus befallen sein!). Unter Windows sollte die Reinigung so schnell wie möglich geschehen. Die Viren-Scanner bieten meist eine Beschreibung für den gefundenen Virus. Diese bietet Anhaltspunkte, was man unbedingt vermeiden sollte, was man tun kann und was im Speziellen gefährdet ist (Beschreibung mit der ggf. angelegten Sicherung der wichtigen Daten abgleichen...). Quelle: OE-FAQ