

E-Mail Sicherheit - immer mehr erforderlich!

Es wird täglich immer schlimmer, dass dubiose Gestalten hinter Bildschirmen im Internet sich etwas Neues einfallen lassen, um schädliche Funktionen durch das Internet zu transportieren.

Zum einen werden Computerviren, Computerwürmer, schädliche Skripte aber auch Dialer direkt per E-Mail verschickt und in vielen Fällen ist somit ein Schaden bereits vorprogrammiert.

Zunächst einmal ist es grundsätzlich wichtig, dass man einige Grundregeln für den Umgang mit E-Mails beachten sollte.

Einer E-Mail die von einem Absender kommt den man nicht kennt sollte man grundsätzlich skeptisch gegenüber stehen.

Niemand weis genau was für eine Absicht dahinter steckt.

Es könnte sich um eine SPAM Mail handeln, aber auch um einen Virus, Wurm oder einer HTML-E-Mail mit einem schadhaften Skript.

Zum anderen sollte man schauen welcher Betreff angegeben ist, denn in den meisten Fällen kommt SPAM als englischer Betreff an und sofern man keine Freunde in Amerika oder England hat, ist es schon ein Grund diese E-Mail zu löschen.

Natürlich wird auch in vielen anderen Ländern englisch gesprochen, jedoch wissen Sie am besten in welcher Sprache mit Ihnen kommuniziert wird.

Weiterhin sollte man grundsätzlich Dateianhänge zunächst einmal nicht öffnen, bevor man nicht sicherstellen kann, ob man von der Person tatsächlich eine Datei geschickt bekommen sollte oder man genau diese Datei im Anhang angefordert hat.

Was kann man nun genau tun, um sich in seinem Posteingang etwas wohler zu fühlen und nicht permanent Würmer, Viren oder andere Schädlinge zu bekommen?

Unter der Voraussetzung das es sich um ein Windows E-Mail Client handelt, gebe ich ein paar Tipps und Tricks ab, um sich etwas besser zu schützen.

In einem [Artikel vom 2.10.03](#) beschreibe ich unter anderem die Methode, wie man sich zunächst einmal direkt auf dem lokalen Computer vor SPAM etwas schützen und den Posteingang automatisch bereinigen kann.

SPAM ist derzeit ein sehr lästiges Problem, was jedoch am schlimmsten Unternehmen mit einem Netzwerk und vielen E-Mail Adressen trifft.

Hierzu sei angemerkt, dass Mitarbeiter solcher Unternehmen stets eine private E-Mail Adresse nutzen sollten wenn sie in Foren aktiv sind und/oder sich in Gästebüchern verewigen möchten.

Zum einen ist die geschäftliche Adresse dann doch etwas geheimer und schwirrt nicht quer durch das Internet und zum anderen ist eine geschäftliche E-Mailadresse zur betrieblichen Kommunikation gedacht.

E-Mail Sicherheit, geht das überhaupt?

Als erstes sollte man versuchen sich HTML-Formate in E-Mails grundsätzlich abzugewöhnen, da hier bereits die Gefahr besteht, dass direkt in HTML eingebettete Skripte oder Programme eine Schadensfunktion beinhalten.

Ein solches Skript oder Programm ist durch die HTML Funktion dann nicht mehr unmittelbar zu sehen und ist eine E-Mail ersteinmal geöffnet, ist auch ein eingebettetes Skript automatisch gestartet.

In einigen Artikeln habe ich bereits von einem Plug In gesprochen, das automatisch ankommende E-Mails vom HTML Format ins reine Text Format ändert.

Somit kann schon einmal gewährt sein, dass keine Skripte direkt ausführbar sind.

Weiterhin ist somit auch einsehbar, woher aus einer HTML formatierten E-Mail die Bilder stammen oder eventuell auch Musik die eingebettet wurde.

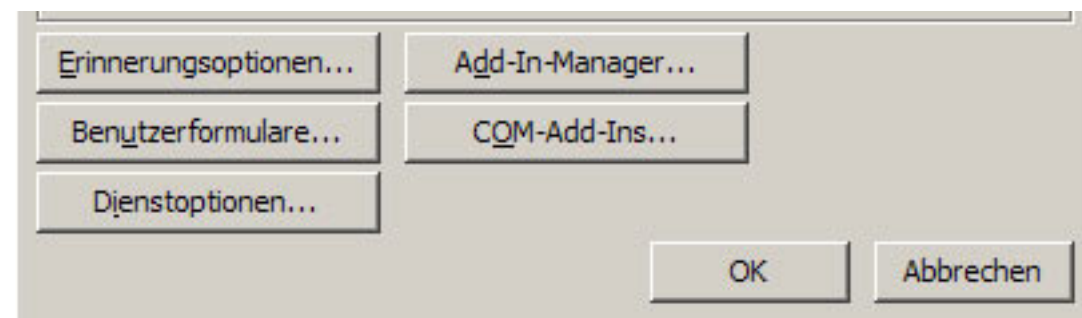
Anhand von [Outlook 2003](#) erkläre ich kurz, wie es schnell und einfach möglich ist das Plug In einzubetten und damit zu arbeiten.

Als erstes sollte man sich das kleine Plug In downloaden: <http://ntbugtraq.ntadvice.com/>.

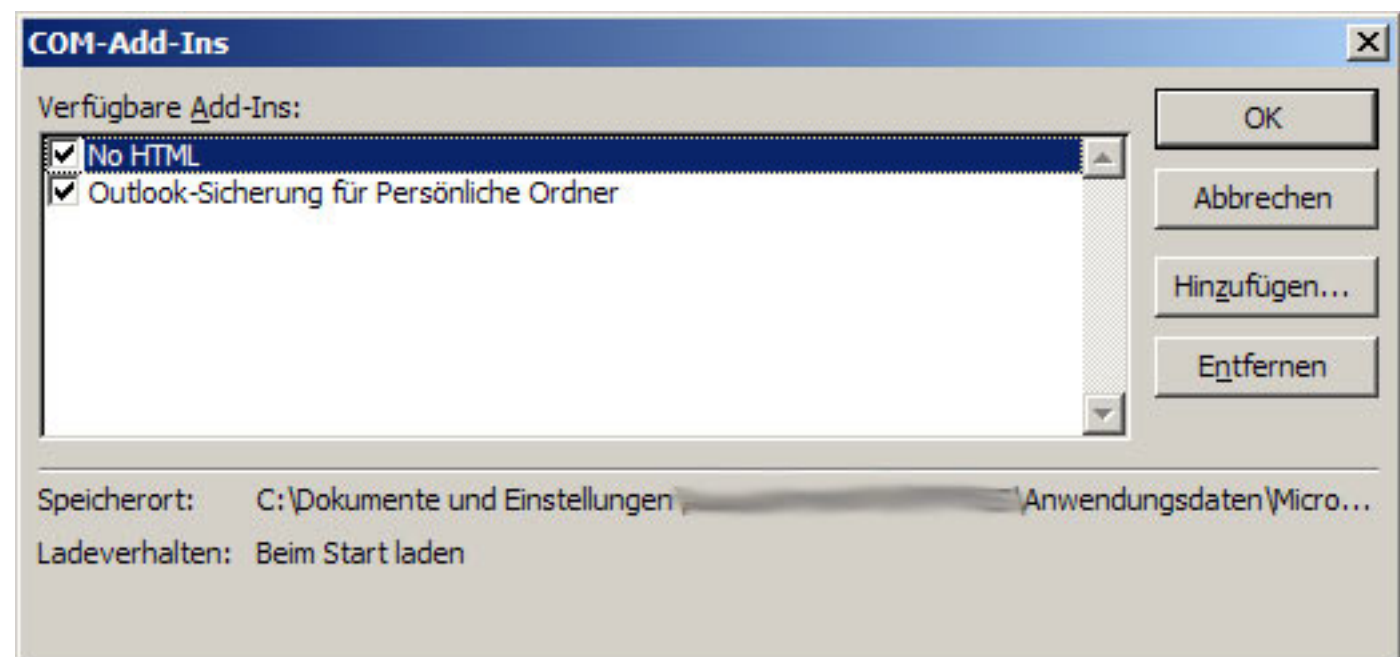
Anschliessend entpackt man das ZIP Files was man geladen hat und legt es entsprechend in den Unterordner für Microsoft Outlook.

Im Normalfall hier zu finden: [/Dokumente und Einstellungen/Username/Application Data/Microsoft/Addins](#) oder unter [/Dokumente und Einstellungen/Username/Application Data/Microsoft/Outlook/Addins](#).

Nun wechselt man in sein Outlook und geht in das Menü EXTRAS und klickt auf OPTIONEN. Anschliessend wechselt man in die Karteikarte WEITERE und findet die Button für COM-Add-Ins (Add-In-Manager) vor sich:



Nachdem der Add-In-Manager geöffnet wurde, kann man das Plug-In NoHTML direkt dort hineinlegen.



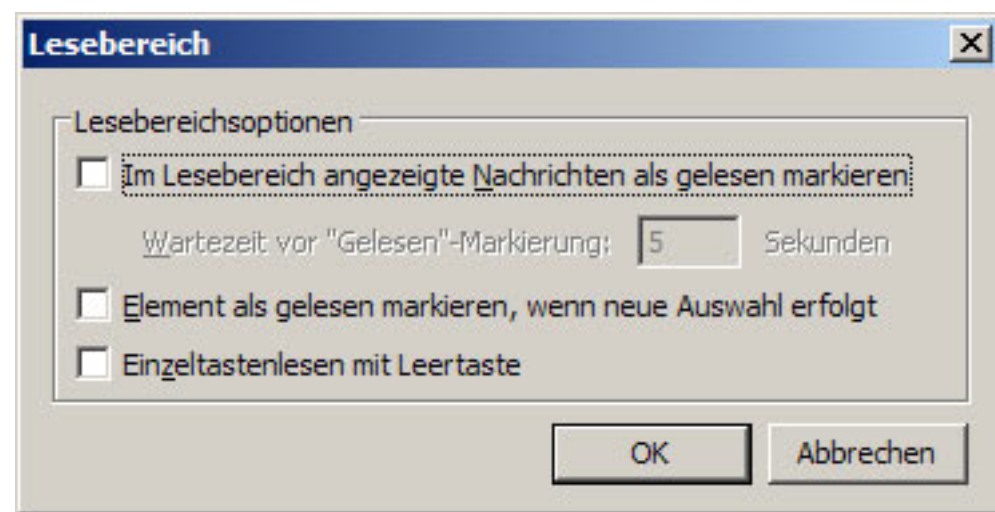
Man geht auf hinzufügen, sucht im oben besagten Ordner die Datei NoHTML.dll und fügt diese direkt hinzu und bestätigt das ganz mit ok.

Schon ist man zunächst einmal von HTML E-Mails in Outlook befreit und kann sich etwas sicherer fühlen.

Im Weiteren ist nun darauf zu achten, dass durch Outlook keine E-Mails automatisch geöffnet werden wenn eine neue Auswahl innerhalb von Outlook erfolgt.

Hierzu kann man eine einfache Einstellung vornehmen, die genau dieses "Problem" unterbindet.

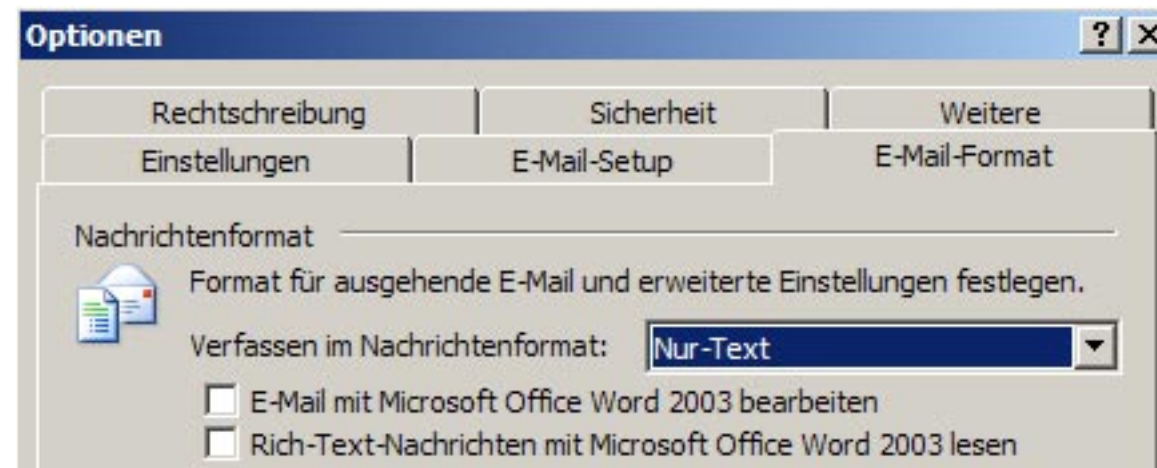
Im Menüpunkt WEITERE befindet sich ebenfalls ein Button, der dafür zuständig ist: Lesebereich. Den Button einmal betätigen und alle Kästchen sollten deaktiviert sein:



Es wird gewährleistet, dass man als Benutzer von Outlook nun selbst entscheiden kann, wann eine E-Mail als geöffnet gilt und wann nicht.

Was man nun von anderen erwartet, kann man selbst natürlich auch praktisch gleich umsetzen. Hierzu empfehle ich, E-Mails nur im reinen Text Format zu erstellen und auf WORD als E-Mail Schreibprogramm zu verzichten.

Im Menü EXTRAS und dann OPTIONEN befindet sich der Reiter (Karteikarte) E-Mail Format und nimmt die Haken einfach raus.



Was aber nicht zu vergessen ist, die Dateianhänge sollten natürlich sichtbar sein.

Die Sichtbarkeit von Dateianhängen ist oftmals von den Grundeinstellungen abhängig die bei Windows voreingestellt sind.

Änderungen vornehmen:

Klicken Sie dazu einfach mit der linken Maustaste doppelt auf das Arbeitsplatz-Icon auf dem Desktop und rufen anschliessend das Menü "Extras" und dort die "Ordner-Optionen" auf.

Hier entfernen Sie das Häkchen an "Dateinamenerweiterungen bei bekannten Dateitypen ausblenden".

Weiterhin sollten Sie das Häkchen an "Geschützte Systemdateien ausblenden" entfernen.

Zum Schluss setzen Sie das Optionsfeld auf "Alle Dateien und Ordner anzeigen".

Nun werden auch alle Dateiendungen angezeigt und wie im Falle des einen oder anderen Wurms, sieht man schon das es sich hierbei um eine doppelte Endung handelt: testdatei.txt würde man normal

sehen, jetzt kann es jedoch schon wieder anders aussehen: testdatei.txt.com.

Es handelt sich um die gleiche Datei, nur das die Datei komplett mit der Endung angezeigt wird und so erkennbar ist, dass es sich um eine ausführbare Datei handelt.

Die neueren Versionen von Outlook unterbinden das Ausführen und Empfangen von ausführbaren Dateien.

Nachdem schon mal die Hausmittel von Outlook genutzt wurden, kann man sich dem SPAM zuwenden und eine Möglichkeit suchen, dem Herr zu werden.

Dazu empfehle ich das Plug In [SPAM BAYES](#) für Outlook, dass ebenfalls bei Outlook 2003 voll funktionstüchtig ist.

Ist das Plug In erst einmal installiert, so benötigt es einige wenigen Tage um Spam Mails entsprechend zu analysieren und dann im Verlaufe der weiteren Tage bereits die SPAM Mails automatisch auszusortieren.

Die Arbeitsweise von Spambayes habe ich in einem vorhergehenden Artikel beschrieben: [Spammer werden immer dreister - Spam den Kampf ansagen](#) // German-Secure.

Weiterhin kann ich empfehlen, die Office Produkte von Microsoft entsprechend immer mit den neuen Versionen, Patches und Updates zu versorgen!

Computerviren und Computerwürmer sind nach wie vor drastisch unterwegs und verstopfen die Internetwege, daher ist natürlich ein Virens Scanner unerlässlich, der jede eingehende E-Mail direkt scannt und auf Viren und Würmer überprüft.

Auf den Internetseiten von Rokop-Security werden in einer extra Rubrik die Tests von Anti-Virusprogrammen bereit gestellt.

Homepage: [Rokop Security Anti-Virus](#) Software.

Es gibt sicherlich noch viele Möglichkeiten, die ich unmöglich hier gebündelt aufzeigen kann. Weitere Hilfen gibt es auf den Verweisen am Ende des Artikels.

Alternativ besteht natürlich auch unter Windows jeder Zeit die Möglichkeit, mit anderen E-Mail Programmen als mit Outlook oder Outlook Express zu arbeiten.

Beispielsweise kann man mit GeMail oder auch mit Pegasus Mail arbeiten, da beide Programme derzeit noch in deutscher Sprache erhältlich sind.

Ebenfalls ist TheBat als E-Mail Client empfehlenswert.

Hilfen, Verweise, Links:

Rokop Security: <http://www.rokop-security.de>

Trojaner-Info: <http://www.trojaner-info.de>

German-Secure: [SPAM den Kampf ansagen!](#)

German-Secure: [SPAM - Datenmüll bekämpfen, weitere Tipps und Tricks!](#)

Security Info Schweiz: <http://www.securityinfo.ch>

Lernen im Internet: [E-Mail Adressen im Netz verstecken](#)

Hacking Intern: [Kapitel 7, ab Seite 397: 0190-Dialer von seriös bis illegal & Spam und Flaming - wenn das Postfach platzt](#)

E-Mail Security Test: [GFI Sicherheitstest](#)

Danke für die Hilfe: Mr. @Feel

Beste Grüße, Marko Rogge // IT-Sicherheits Berater

German-Secure :: IT-Sicherheitsberatung

21.01.2004