

Merkblatt zu Dialern (Telefon-Einwahl-Programmen)

Neuerdings treten diese in Massen und diversen Variationen auf, sowohl als E-Mail-Anhänge, als auch als harmlos getarnte Datei-Downloads.

Voraussetzungen:

Man besitzt einen PC, welcher über eine Wählleitung (gewöhnliche Telefonleitung) mittels analogem Modem oder digitalem ISDN-Adapter mit dem Internet verbunden werden kann.

Besitzer von Routern oder andern Geräten, bei denen die Telefonnummer des Internet-Providers (z.B. Bluewin) fest einprogrammiert ist, sowie Internetuser welche über ADSL oder Kabel-Modem verfügen, erfüllen die Voraussetzungen nicht.

Was ist geschehen ? (Symptome)

Man erhält eine stark überhöhte Gebührenrechnung z.B. von der Swisscom, verlangt einen Verbindungsnachweis und steht vor einem Rätsel:

- Verbindungen an eine 0906 xxx xxx –Nummer (Unterhaltung) mit Minutentariifen von 4 Fr. und mehr,
- Verbindungen ins Ausland,
- Verbindungen an völlig unbekannte Ziele

Mögliche Ursache:

Sofern der PC im fraglichen Zustand mit dem Internet verbunden war, dürfte die Ursache ein sogenannter Dialer sein.

Dialer – Hintergrundinformation:

Dialer sind kleine Programme, die benutzt werden, um über eine Telefonleitung die Einwahl ins Internet zu ermöglichen.

Sie verhalten sich also prinzipiell ähnlich wie ein DFÜ-Icon (rechts) zur Einwahl auf die Telefonnummer (z.B. 0840840222) des Providers (z.B. Bluewin) und es entstünden auch keine Probleme, wenn alle Vorschriften eingehalten würden, was leider selten der Fall ist.



Denn offiziell, d.h. gemäss Verordnung SR 784.101.113 / 2.8 des BAKOM, gelten strenge Anforderungen an diese (Auszug):

Werden 090x-Nummern für die Verrechnung von Internet- oder Onlinediensten verwendet (insbesondere PC-Dialer), muss die Inhaberin der Nummer Folgendes sicherstellen:

- dauernde Anzeige der auflaufenden Verbindungsgebühren auf dem Bildschirm des Benutzers
- Anzeige immer im Vordergrund mit einer minimalen Schriftgrösse von 14 Punkten, auch wenn der Benutzer die Eintrittsseite durch Auswahl weiterer Internetseiten verlässt (diese Schrift hat 12 Punkte)
- Unmittelbarer Abbruch der (teuren) Verbindung beim Schliessen des Browser-Programmes durch den Benutzer bzw. bei Beendigung der Kommunikationssitzung.

- Die auf dem Endgerät des Benutzers (PC) gespeicherte DFÜ-Verbindung für den Zugang zu Internet- oder Onlinediensten über eine 090x-Nummer darf nicht ohne ausdrückliche Kenntnisnahme und Zustimmung des Benutzers als Standardverbindung eingerichtet werden.
- Personen unter 16 Jahren darf kein Zugang zu Diensten mit pornografischen Inhalten gemäss Artikel 197 Strafgesetzbuch gewährt wird.

Bei einem Dialer ist normalerweise die gewählte Telefonnummer dem Benutzer ebenso unbekannt wie die anfallenden Telefongebühren, welche beliebig hoch sein können. Denn während bei der gewöhnlichen Verbindung über einen Provider wie Bluewin der Lokaltarif (z.Z. max. CHF 4 pro Stunde) zur Anwendung kommt, kann die Einwahl über einen Dialer locker 100 (in Worten hundert) mal teurer sein. Zudem können sie als Spiel oder (animierte) Grafik getarnt sein. Extrem perfide Tricks und Täuschungsmanöver zur Umgehung von Sperrern etc. werden zunehmen. Auch Viren-artige Verbreitung ist denkbar.

Vorgesehene „ursprüngliche“ Funktion eines Dialers:

Zum Abruf von "erotischen" Angeboten aus dem Internet benötigt man häufig einen Dialer, dieser muss aber IMMER zuerst heruntergeladen und gestartet werden. Nach dem Start wird die aktuelle Telefonleitung zum Internet-Provider aufgehängt und die im Dialer gespeicherte Telefonnummer gewählt.

Bei einem analogen Telefonanschluss beginnt dann das ca. 30 s dauernde Einwahlprozedere des Modems, welches auch akustisch festgestellt werden kann. Bei einer digitalen ISDN-Anlage geschieht alles innerhalb von 1 Sekunde - man hat also keine Chance dies wahrzunehmen.

Mögliche Seiteneffekte:

Dialer können beliebige unerwünschte Seiteneffekte (z.B. Absturz, Festplatte wird gelöscht etc. etc.) auslösen und beliebig getarnt sein! Auch ist es möglich, dass sie sich immer wieder von selbst starten und nur schwer entfernen lassen.

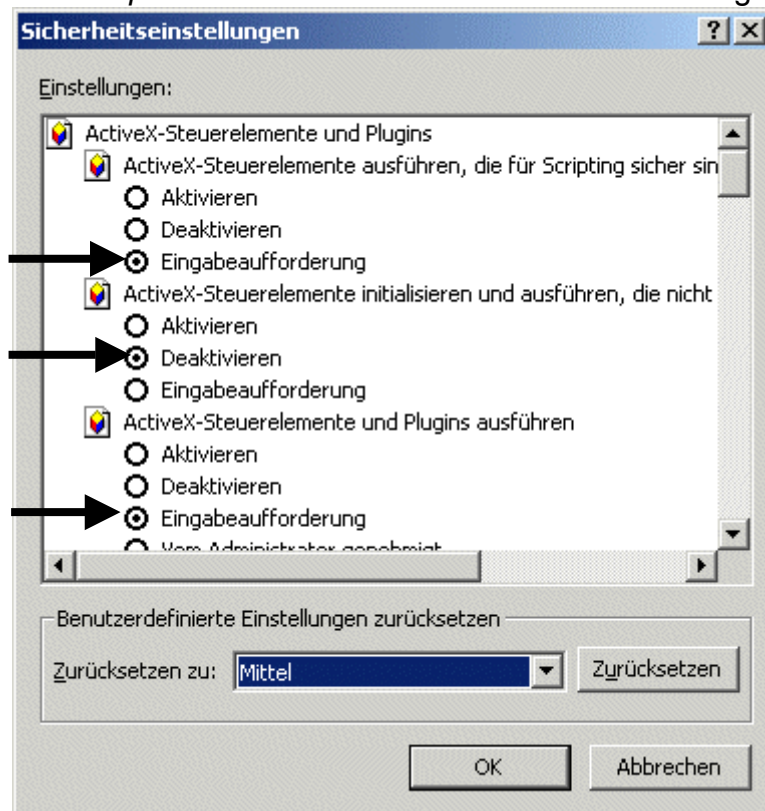
Generelle Vorsichtsmassnahmen:



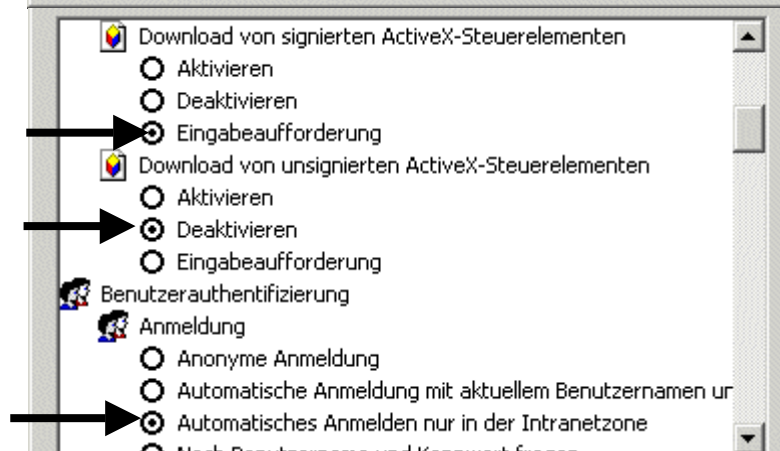
Sicherheitswarnungen immer beachten und grundsätzlich mit „**Nein**“ beantworten!

Damit Sicherheitswarnungen überhaupt erscheinen, müssen die Sicherheitseinstellungen im Browser (Microsoft Internet Explorer) korrekt sein.

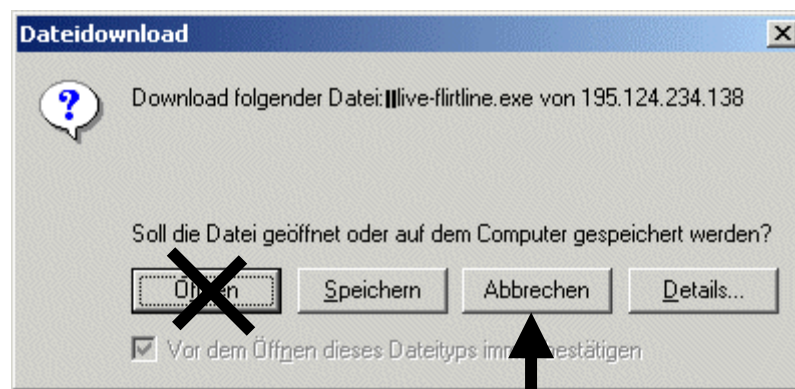
Diese können über das Menü *Extras – Internetoptionen ... Sicherheit* und die Taste *Stufe anpassen..* kontrolliert werden. Die Einstellungen sollten wie folgt gesetzt sein.



ActiveX-Steuerelemente sollten NIE generell aktiviert werden, da sonst unbemerkt beliebige Programme installiert werden können.



Weitere relevante Einstellungen



Erscheint (unvermutet) der Datei-Download-Dialog sollte man **grundsätzlich** die **"Abbrechen"-Taste** betätigen. So können keine unliebsamen Überraschungen z.B. beim Erhalt der Telefonrechnung auftreten.

Bei E-Mail-Anhängen ist dasselbe Vorgehen empfehlenswert, ebenso im Hinblick auf allfällige Viren-Infektionen.

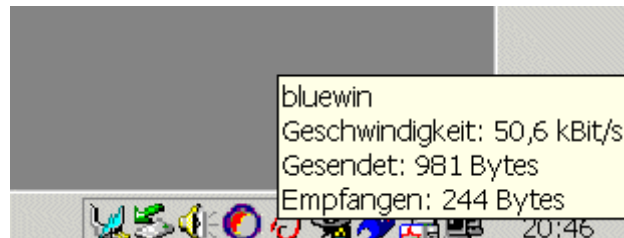
Beim Datei-Download-Dialog sollte **NIE die "Öffnen"-Taste** angeklickt werden! Wird ein Datei-Download gewünscht, sollte die Datei **IMMER** zuerst gespeichert werden, damit der aktivierte Virens Scanner (mit den neusten Signaturen) die Möglichkeit hat, einen allenfalls versteckten Virus zu entdecken.

Eine **Sperre abgehender Verbindungen** auf 0906x-Nummern kann über die Gratisnummer 0800 800 800 angefordert werden und ist sinnvoll, aber bei Nichtbeachtung obiger Vorsichtsmassnahmen nicht ausreichend.

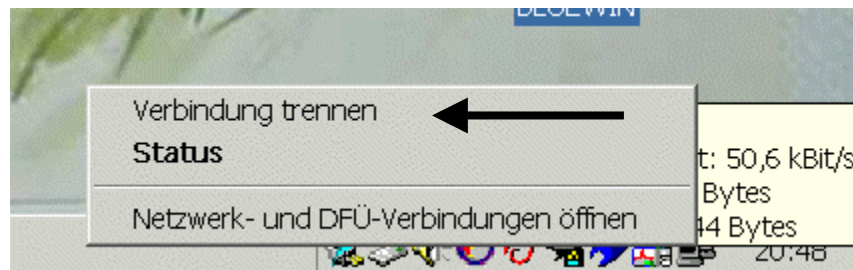
Was ist unmittelbar zu tun, wenn man in die Falle getappt ist:

Verbindung sofort trennen - über das Symbol mit den 2 Bildschirmen, rechts unten am Bildschirm neben der Uhr.

Falls dieses Symbol bei einem böseren Dialer überhaupt vorhanden ist.



Bleibt man mit der Maus auf dem Symbol stehen, erscheinen die Verbindungsdaten. So kann man auch sofort feststellen, ob man mit dem eigenen Provider, z.B. Bluewin verbunden ist oder nicht.



Zum Trennen die **rechte Maustaste** auf dem Symbol mit den **2 Bildschirmen** klicken und anschliessend **Linksklick** auf **Verbindung trennen**.

Falls das Symbol mit den 2 Bildschirmen am untern, rechten Rand des Bildschirms nicht auffindbar ist, dann muss das Modem bzw. der ISDN-Adapter **SOFORT** manuell ausgeschaltet werden.

Falls das Modem oder der ISDN-Adapter keinen Schalter besitzt, dann muss die **Kabel-Verbindung** zwischen Modem bzw. ISDN-Adapter und **Telefonanschlussdose** aufgetrennt werden (Kabel ausstecken).

Was ist zu tun, damit der Dialer nicht mehr aktiv werden kann?

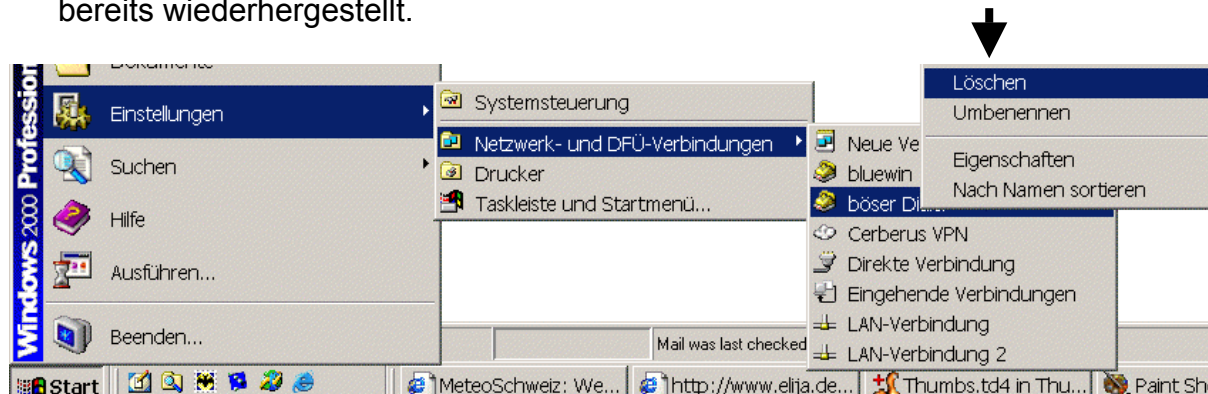
Vorab: ist erheblicher finanzieller Schaden entstanden, sollte zu Beweis Zwecken eine möglichst vollständige Sicherheitskopie (Backup) des Systems gemacht werden. Erst danach sollte man über eine Entfernung oder Deaktivierung nachdenken.

Zur Beseitigung gibt es verschiedene Ansätze.

- Die komplette Löschung des Dialerprogramms und der zugehörigen Verbindungsdaten, sowie ev. weiterer Dateien. Das erste Problem ist das

Auffinden und Identifizieren und das zweite ein möglicher Beweisnotstand, der durch die Entfernung entstehen kann

- Die dauerhaften Inaktivierung: Diese kann ev. bewerkstelligt werden, indem die böartige "DFÜ-Verbindung" im Menü "Einstellungen / Netzwerk und DFÜ-Verbindungen" entfernt wird (rechte Maustaste auf der Verbindung betätigen). Höchstwahrscheinlich ist aber die Freude von kurzer Dauer und die ursprünglichen böartigen Verbindungsdaten nach dem nächsten Start des PCs bereits wiederhergestellt.



Genau wie gegen Computerviren-Infektionen sind auch gegen Dialer noch keine Patentkräuter gewachsen. Gewöhnlich nisten sich diese gut getarnt tief im System ein. Je unseriöser die Absichten eines Dialer-Anbieters, desto schwieriger dürfte die Entfernung werden.

Hinweis auf Folgeschäden: Treten nach einem solchen Zwischenfall und trotz (vermeintlicher) Stilllegung des Dialers seltsame Symptome auf wie:

- unbeabsichtigte Verbindungsversuche zum Internet
- unbeabsichtigter Aufruf von Sex-Seiten
- seltsame Fehlermeldungen

dann muss der böartige Dialer von einem Fachmann entfernt werden.

Wie könnte ein Schutz aussehen ?

Neben den bereits erwähnten Vorsichtsmaßnahmen einer korrekten Konfiguration der sicherheitsrelevanten Einstellungen des PCs, der **kostenlosen Sperre der 0906er-Telefonverbindungen bei der Swisscom über die Gratisnummer 0800 800 800**, Dialer-Blocker Software etc. wäre es auch möglich auf Windows zu verzichten und damit Dialern und anderen Arten Malware fast keine Chancen zu geben.

Keine Chancen hätten Dialer, wenn das Modem oder der ISDN-Adapter nur bestimmte vorgegebene Nummern wählen könnte. In Deutschland gibt es inzwischen ein Gerät genannt **Dialer Blocker**, welches zwischen das analoge Modem bzw. den ISDN Adapter und die Telefondose geschaltet, einen 100% Schutz gewährleistet, da nur 8 vom Benutzer vorgegebene Telefonnummern durchgeschaltet werden. Das Gerät kann für 30 bzw. 40 € bei www.conrad.de bestellt werden.

Sehr gute Informationen zum gesamten Thema liefert das Web unter <http://www.dialerschutz.de/> - auch für die Schweiz. Unter <http://www.e-ofcom.ch/liste> kann die Liste der Betreiber von 0906er Nummern etc. abgefragt werden.