Virenschutz - Informationen zu Ihrer Sicherheit

Virenschutz ist für jeden Computer-Nutzer ein absolutes Muss.
Auf dieser Seite finden Sie nützliche Tipps, Ratschläge für den Ernstfall und viele interessante Links zu Anti-Viren-Seiten im Web.

Was Sie auf jeden Fall tun sollten

- **Verwenden Sie keine einfachen Passwörter**

Viele Angriffe von außen auf PCs sind deshalb erfolgreich, weil die eindringende Software das Administrator-Passwort erraten kann. Da auf Systemen mit Windows XP/Vista/7 in aller Regel der Benutzer „Administrator“ vorhanden ist, ist vor allem dieser Benutzername das Angriffsziel. Das Angreifer-Programm versucht sich einfach mit Hilfe eines Wörterbuches als Administrator am betreffenden Opfer anzumelden. Wenn dies gelingt, wird oft das Passwort geändert, sodass der Eigentümer sich nicht mehr als Administrator anmelden kann und nur mit großer Mühe oder unter Verlusten das System wieder in die Hand bekommt. Solche „gehackten“ PCs werden gerne als Server für den illegalen Datenaustausch missbraucht.

- **Aktualisieren Sie regelmäßig Ihr Betriebssystem**

Einige Schadprogramme nisten sich in Ihrem System ein, ohne den Passwortschutz (s.oben!) durchbrechen zum müssen, indem sie Sicherheitslücken des Betriebssystems ausnutzen, sobald es über das Internet erreichbar ist. Dem PC genügt also in solchen Fällen einfach nur die Internet-Verbindung, um infizierbar zu sein. Dagegen können Sie sich dann schützen, wenn der Hersteller (in unserem Fall Microsoft) ein Programm zur Fehlerbereinigung (ein sog. Patch) herausbringt. Deshalb ist es dringend ratsam, die Update-Seiten von Microsoft regelmäßig aufzusuchen oder das Betriebssystem auf automatische Aktualisierung einzustellen. Sie können, um Kontrolle über die Aktualisierungen haben, die automatische Aktualisierungsfunktion so einstellen, dass Sie vor dem Herunterladen oder vor der Installation gefragt werden und dann entscheiden können, welche Patches Sie ins System übernehmen wollen.

- **Installieren Sie auf Ihrem PC ein Antiviren-Programm**

Das Rechenzentrum bietet für alle PCs in der Uni Freiburg kostenfrei ein Installationspaket der **Antivirensoftware Sophos** Antiviren-Software an.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit seiner Website **BSI für Bürger** umfangreiches Informationsmaterial auch zu Viren, Würmern und ähnlichen Schadprogrammen zur Verfügung.

Auf der **Virenschutz-Infoseite** können Sie sich unverbindlich über freie und kostenpflichtige Angebote von Schutz-Software informieren.

Nach einer **Untersuchung der Zeitschrift c't** vom Februar 2010 ist es am sinnvollsten, den Firewall-Schutz, den Windows seit XP mit Service Pack 3 anbietet in Verbindung mit einem reinen Anti-Virus-Programm zu nutzen. Aufwändige „all in one“ - Lösungen versprechen meist mehr, als sie halten können und belasten den Rechner über das nötige Maß.

- **Sorgen Sie dafür, dass das Programm regelmäßig aktualisiert wird**

Hierzu werden Sie bei der Installation von Sophos automatisch aufgefordert. Wenn Sie andere Software installieren bzw. schon installiert haben, ist ein automatisches Update der Vireninformationen in den meisten Fällen möglich. Je öfter, desto besser!

- **Sorgen Sie dafür, dass ein speicherresidenter Virenwächter läuft**

Sie sollten kein Antiviren-Programm installieren, das diese äußerst wichtige Komponente nicht anbietet. Sie sollte grundsätzlich bei Systemstart automatisch anlaufen. Damit haben Sie für die gesamte Sitzungszeit eine Überwachung aller von einem Datenträger gelesenen und/oder auf einen Datenträger geschriebenen Dateien. Infizierte Downloads können auf diese Weise erkannt werden.

Was Sie auf keinen Fall tun sollten

- **Öffnen Sie niemals Dateien ohne Kontrolle durch ein Antiviren-Programm**

Vor dem Öffnen sollten Sie die Programmdateien (ggf. nach dem Entpacken) auf Viren überprüfen. Falls Sie einen Virenwächter installiert und aktiviert haben, geschieht dies immer beim Speichern, Starten oder Öffnen von Dateien bzw. Programmen.

- **Öffnen Sie niemals Dateianhänge direkt aus dem Mailprogramm heraus**

Ein bewusster, vorsichtiger Umgang mit dem Internet ist eine der wichtigsten Voraussetzungen für die Sicherheit Ihrer Daten. Unaufgefordert zugesandte Mails, insbesonders mit Anhängen, sind mit Vorsicht zu genießen.

ACHTUNG: Firmen versenden nie unaufgeforderte Programmpakete zur Aktualisierung oder Fehlerbehebung. Selbst wenn die Anhänge harmlose Dateinamenserweiterungen zu besitzen scheinen, hinter denen man nie und nimmer Viren vermuten würde, ist Vorsicht geboten.

Auf jeden Fall sollten Sie bei einem aktiven und aktuellen(!) Virenwächter im Hintergrund die Anhänge zunächst abspeichern, bevor Sie sie öffnen.

Manche Antiviren-Produkte schließen auch die Überprüfung der Mails und ihrer Anhänge direkt beim Herunterladen vom Mailserver ein. In diesem Fall kann man sich das temporäre manuelle Abspeichern der Dateien sparen.

- **Vermeiden Sie das Surfen im Internet, wenn Sie als Administrator angemeldet sind (Windows)**

Falls ein Angriff auf Ihren PC gelingt, sind die Möglichkeiten des Angreifers deutlich eingeschränkt, wenn Sie zu diesem Zeitpunkt mit möglichst wenig Rechten angemeldet sind.

- **Vertrauen Sie niemandem, dessen Vertrauenswürdigkeit Sie nicht überprüft haben**

Lassen Sie sich nicht einfach von seriös aussehenden Versprechungen oder vermeintlich günstigen Software-Angeboten in eine Falle locken. Suchen Sie im Zweifel mit Hilfe von Suchmaschinen nach Hintergrundinformationen über die Quelle und prüfen Sie kritisch!

Bei Mails müssen Absenderangaben nicht unbedingt der Wahrheit entsprechen. Fälschungen im Adresskopf von Mails sind überaus leicht herzustellen. Beispielsweise setzen die sogenannten **Phishing-Mails** auf die Vertrauensseligkeit der Mail-Anwender.

Vorsicht: Haben Sie in einem lokalen Ordner des PC eine infizierte E-Mail gespeichert, kann Ihnen beim Einsatz eines Antiviren-Programmes der totale Verlust des betreffenden Ordners drohen. Der Grund: Die geläufigen Mailprogramme (z.B. Mozilla Thunderbird oder Outlook) pflegen alle Mails eines Ordners in einer Datei zu sammeln. Wird darin eine Virus-Sequenz entdeckt, wird die ganze Datei als verseucht behandelt und ggf. entsorgt.

Fall 1: Ihr PC ist das Ziel eines Infektionsversuches

Falls Sie von Ihrem Antivierenprogramm gewarnt werden, dass ein Ihnen zugestellter elektronischer Brief virusinfiziert ist, oder Sie aus anderen Gründen den Verdacht haben, mit einem E-Mail-Virus beehrt worden zu sein, empfehlen wir folgendes Vorgehen:

- Identifizieren Sie den Brief und seinen Absender
- Stellen Sie fest, um welchen Dateityp es sich handelt, der den Virus enthält (.EXE, .VBS, .PIF). Üblicherweise befindet sich das Machwerk im Anhang (Attachement).
- Eine Besonderheit: Manche Mailprogramme (z.B. Eudora) extrahieren die Anhänge automatisch in ein von Ihnen festzulegendes Verzeichnis. Dann sehen Sie dort nach den neuesten Dateien.
- Das einfache Abspeichern eines infizierten Attachements ist ungefährlich. Sie müssen lediglich darauf achten, dass Sie es - je nach Typ - nicht öffnen oder ausführen.
- Bereits der Doppelklick auf das Attachement-Symbol in der Mail kann die Ausführung des Virencodes veranlassen. Hier müssen Sie also besonders vorsichtig sein.
- Löschen Sie den Brief und den eventuell extrahierten Anhang.

Es ist sicher eine gute Sache, wenn Sie den Absender davon in Kenntnis setzen, dass ein von ihm versandter Brief infiziert war.

Fall 2: Ihr PC ist die vermutete Quelle eines Infektionsversuchs

Falls Sie eine (meist automatisch generierte) Nachricht erhalten, dass Ihre Mail (sie wird dabei meist im Anhang aufgelistet) nicht abgeliefert werden konnte, Sie aber sicher sind, an die besagte Adresse keine solche Mail gesandt zu haben, kann es sich um folgende Situationen handeln:

- Ihr PC ist infiziert und verschickt ohne Ihr Wissen infizierte Mails an Adressen, die in Adressbüchern auf dem PC gefunden werden. Dabei hat „Ihr Virus“ in seltener Ehrlichkeit die korrekte Absenderadresse eingesetzt.
  Sie sollten umgehend etwas gegen die Infektion unternehmen und ein gutes

Antivirenprogramm installieren!
- Ein anderer PC irgendwo auf der Welt, dem Ihre Mailadresse bekannt ist, trägt einen Computervirus und verschickt infizierte Mails, wobei in der Regel die Absenderadresse gefälscht wird. Im konkreten Fall wurde zur Fälschung Ihre Mailadresse als Absender herangezogen. Gegen diesen Adressdiebstahl sind Sie machtlos. Diese Situation wurde weiter oben bereits erwähnt.
  Zufällig hat nun der versendende Virus eine ungültige/nicht mehr gültige Mailadresse als Ziel eingesetzt und so dafür gesorgt, dass Sie von dem Vorfall unterrichtet wurden.

Hilfe, ich bin infiziert!

Falls Sie auf Gund unerklärlicher Verhaltensweisen Ihres Systems den Verdacht auf Virusbefall haben, finden Sie heraus, ob sich tatsächlich ein Virus festgesetzt hat und um welchen Typ es sich handelt. Sie müssen allerdings damit rechnen, dass nicht alle Infektionen erkannt werden, wenn Sie die Virensuche bei gestartetem infizierten System durchführen. Viele Viren sind - sobald sie gestartet sind - in der Lage, sich wirkungsvoll vor Antivirensoftware zu verbergen.

Bei den Systemen Windows XP oder Vista kann im Infektionsfall guter Rat teuer werden. Vorbeugen ist eben auch hier besser als heilen.

Wenn Sie auch dann nicht mehr weiter wissen, wenden Sie sich einfach an unsere Beratung. Dort wird man weitere Hilfsmittel einsetzen, um Sie beim Lösen des Problems zu unterstützen.

Bekämpfung neuester Viren

Beim Auftreten brandaktueller Viren sind die Vireninformationsdateien nicht immer auf dem neuesten Stand. Deshalb bieten viele Hersteller von Antiviren-Software Spezialprogramme zum Erkennen und Beseitigen allerneuester Viren an.

- **http://www.symantec.com/avcenter/tools.list.html**
- **http://vil.nai.com/vil/stinger**
- **http://housecall.trendmicro.com/de**

Suchmaschinen

Auf den Webseiten der wichtigsten Hersteller von Antiviren-Software finden Sie Suchmaschinen, die Ihnen beim Auffinden von Virenbeschreibungen behilflich sind. Sie sollten beim Suchen an Hand von Virenbezeichnungen beachten, dass die Hersteller u.U. verschiedene Namen verwenden. Deshalb ist es von Vorteil, bei einer misslungenen Namens-Suche auch noch andere Suchmaschinen zu konsultieren. Oft wird in der Virenbeschreibung dann auf alternative Namen hingewiesen.

Einige Hilfen:

- **Sophos**
- **Symantec (Norton)**
- **Network Associates (McAfee)**
- **Trend Micro**

Infos speziell zur Trojaner-Problematik

- **Trojaner-Info: Die deutschen Trojaner-Seiten** - Alles Wissenswerte über Trojaner
- **Trojaner-Board: Diskussionsforum** - Höchst informativ

Sicherheit - Artikelübersicht, Virenschutz - Artikelübersicht