Rechenkraft.net e.V.

Sicherheit bei der Installation von Distributed-Computing-Software auf Computern

Distributed-Computing-Software hilft, ist sicher, stört nicht und bleibt auf Wunsch im Hintergrund. Dennoch sind unbekannte Programme weniger gern gesehen, weil man die Folgen einer Installation nicht absehen kann.
Distributed-Computing-Programme dienen ausschliesslich zu wissenschaftlichen Zwecken und sind von ihrer Art der Installation und Ausführung her nicht problematischer als jede andere Software, die installiert wird.

Rechenkraft.net e.V. programmiert selber keine dc-Clienten, sondern stellt nur Fremd-Programme vor und gibt Hilfestellung bei deren Installation und Benutzung. Diese Programme kommen i.d.R. von renommierten Universitäten wie z.B. der Stanford-University (Kalifornien), der Oxford-University (Grossbritannien) oder Firmen-Zusammenschlüssen wie United Devices (UD).
Von daher ist Rechenkraft.net e.V. nur ein Vermittler, der selber keine Daten von dem jeweiligen dc-Clienten empfangen kann und will.

Grundsätzlich könnte *jede* Software auf einem Computer unbemerkt Daten übertragen. Einige Programme nutzen speziell diese Technik aus, um nach Programm-Updates zu suchen oder sich zu registrieren.
Anhand der folgenden vereinfachten Grafiken (Seite 2) wollen wir zeigen, dass – richtig eingerichtet – dc-Clienten in Hinblick auf heimliche Datenübertragung relativ sicher sind, wenn sie ausschliesslich in ihrer eigenen Benutzer-Umgebung ausgeführt werden.

Heute werden zum Arbeiten überwiegend Betriebssysteme wie Windows 2000, Windows XP, Mac OS X oder Linux zum arbeiten eingesetzt. Jedes dieser Betriebssysteme sind Mehrbenutzer-Systeme (Multiuser-Systeme). Das heisst, dass mehrere Benutzer an ein- und demselben Rechner arbeiten können, ohne sich mit den Programmen oder persönlichen Daten in die Quere kommen zu können, weil jeder Benutzer ein eigenes Passwort hat, mit dem er sich identifiziert. Ebensowenig kann ein Benutzer, nennen wir ihn Holger, Daten eines anderen Benutzers – z.B. Susanne – lesen, verändern oder löschen. Beide Benutzer-Umgebungen sind vollständig voneinander getrennt, sofern das Passwort des jeweiligen Benutzers geheim bleibt.
Angenommen, Holger erstellt mit einem Finanz-Programm (welches er selber startet) einen Geschäftbericht, eine Rechnung oder ähnliches, dann hätte ein Trojaner, welcher im Finanz-Programm versteckt sein kann, die Möglichkeit, z. B. die geschriebene Rechnung auszuspähen und eventuell über das Internet zu versenden. Dagegen kann man sich grundsätzlich nur schwer schützen.
Der Finanz-Trojaner kann jedoch nicht auf Susannes Daten zugreifen, weil er ja von Holger gestartet wurde und somit ausschliesslich in seiner Benutzer-Umgebung läuft.

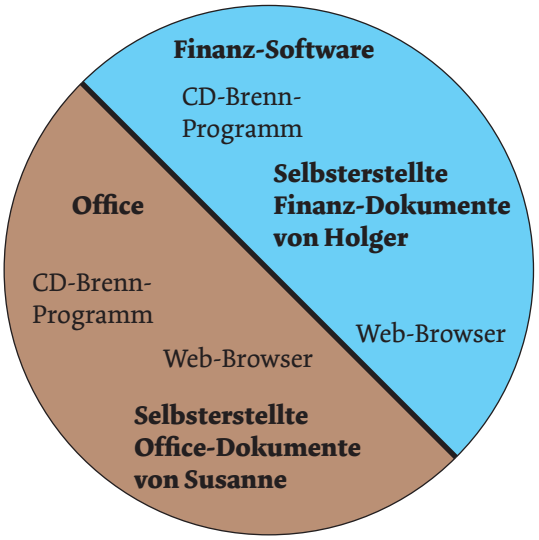
Um einen sicheren Umgang zu gewährleisten, muss ein weiterer Benutzer angelegt werden, nennen wir ihn »Foldhome«. In dieser Benutzer-Umgebung muss die Forschungs-Software (und nur diese!) gestartet werden.
Das Programm kann jetzt keine Daten – weder die von Holger noch die von Susanne – lesen, weil die beiden jeweils ihre eigene Benutzer-Umgebung haben, diese Grenze kann weder unabsichtlich noch mutwillig überschritten werden.

Damit ist auch schon die Antwort gegeben, warum ein dc-Client – sofern in einer eigenen Benutzer-Umgebung gestartet – keine fremden Daten übertragen **kann:**

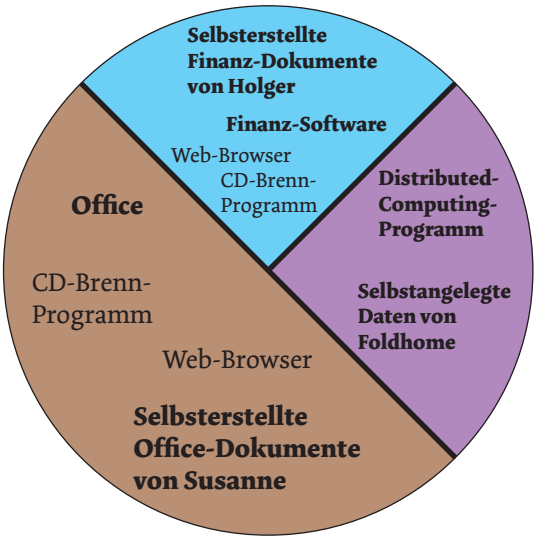
Die folgenden Grafiken verdeutlichen dieses Prinzip noch einmal:

Computer mit nur einem Benutzer (Susanne):
Ein böswillig programmierter Trojaner (der z.B. in einer Office-Software versteckt ist) könnte Susannes damit geschriebene Geschäftsbriefe z.B. über das Internet versenden, weil sich das Programm und die Geschäftsbriefe in ein- und derselben Benutzerumgebung befinden. Dieses Sicherheitsrisiko ist nur schwer vermeidbar.

Computer mit zwei Benutzen (Susanne und Holger):
Ein böswillig programmierter Trojaner (der z.B. in einer Finanz-Software versteckt ist, die nur Holger benutzt) könnte in der jeweiligen Benutzer-Umgebung die selbsterstellten Finanzdaten ausspähen und z.B. über das Internet versenden.
Er kann jedoch **nicht** in Susannes Benutzer-Umgebung eingreifen und ihre Office-Dokumente ausspähen, da Holgers und Susannes Benutzerumgebungen strikt getrennt sind.



Computer mit drei Benutzern (Susanne, Holger und Foldhome):
Neben Susanne und Holger wird vom Administrator ein dritter Benutzer angelegt, nämlich Foldhome. Er hat – wie Susanne und Holger – seine eigene Benutzer-Umgebung und kann somit weder auf Susannes Briefe, noch auf Holgers Finanz-Daten zugreifen und diese ausspähen.
Dieser Distributed-Computing-Client muss nur einmal gestartet werden und braucht dann nicht mehr »angefasst« zu werden.
Er läuft wartungsfrei und unbemerkt im Hintergrund und behindert keinen der anderen Benutzer beim Arbeiten.



Wir hoffen, dass Ihnen das Sicherheits-Konzept der Installation klarer geworden ist und Sie wissen, worauf es bei der Einrichtung und Verwendung von dc-Software auf Firmen-Computern ankommt, um sicher damit arbeiten zu können.
Bei Fragen wenden Sie sich bitte an:
info@rechenkraft.org oder www.Rechenkraft.net

Vielen Dank für Ihre Hilfe bei der Lösung wichtiger Fragen für die Forschung.
Ihr Rechenkraft.net-Team.