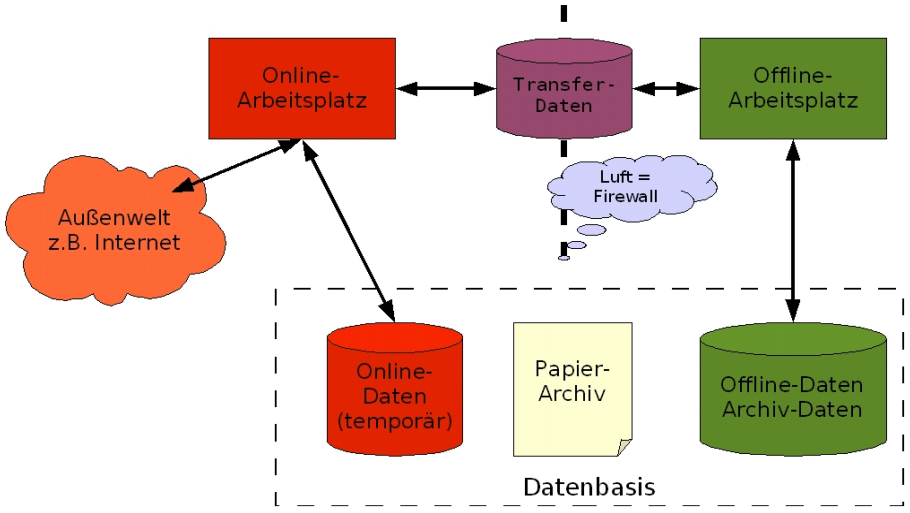
Arbeiten mit dem PC - einfach und sicher.

Ein Vorschlag

Rolf Martens

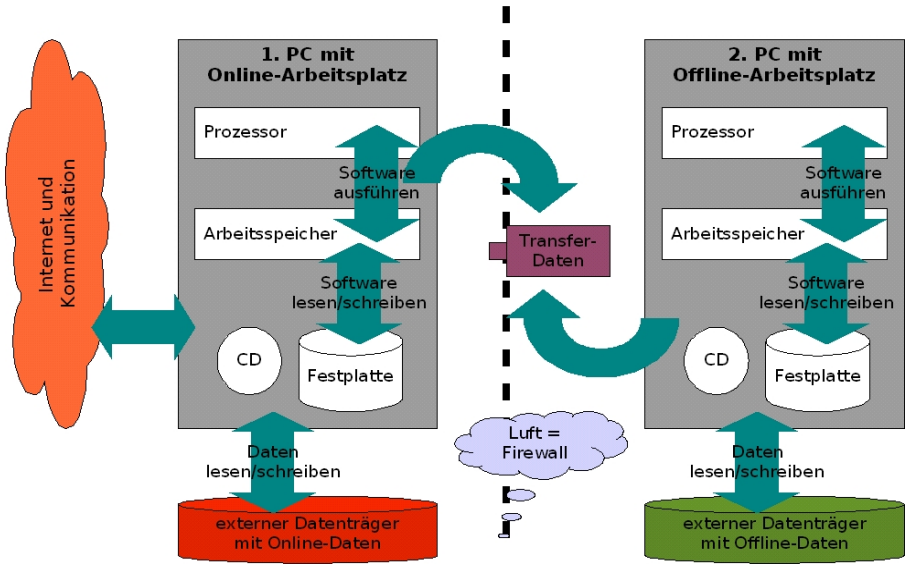
Der typische Personalcomputer in einem kleinen Büro oder Home-Office ist ein PC, mit dem „alles" gemacht wird und in dem „alles" gespeichert wird. Leider entsteht dabei oftmals eine Gemengelage, die zahllose Sicherheitsrisiken und eine irgendwann kaum mehr beherrschbare Kompliziertheit birgt. Dieser „Alles-PC" vermengt austauschbare und (potentiell) riskante Software mit wertvollen und nicht beliebig ersetzbaren Daten, was im Problemfall zu massiven Datenverlusten führen kann. Die Absicherung eines Personalcomputers durch Virenscanner, tägliche Softwareaktualisierungen oder Firewalls hat sich längst zu einem immer wahnwitziger werdenden Räuber-und-Gendarm-Spiel entwickelt, in dem Zeit und Geld der PC-Nutzer verschwendet werden. Angeregt durch die *Sichere Inter-Netzwerk Architektur (SINA)* des Bundesamtes für Sicherheit in der Informationstechnik (BSI) habe ich ein Konzept entwickelt, mit dem ein solcher „Alles-PC" in einen einfach zu handhabenden und sicheren PC-Arbeitsplatz überführt wird. Ziel der Entwicklung dieses Konzepts war es, einige zentrale SINA-Prinzipien mit Open-Source-Software und Standard-Hardware, also ohne Verwendung von teuren Sonderentwicklungen, zu verwirklichen.

Für ein kleines Büro ohne ein „Budget Computersicherheit" in 6-stelliger Höhe gibt es nur eine wirklich sichere Möglichkeit, das Internet zu nutzen und gleichzeitig vertrauliche Daten zu bearbeiten und zu speichern: das Internet wird an einem PC-Arbeitsplatz (***Online-Arbeitsplatz)*** genutzt und die Daten werden auf einem davon physikalisch getrennten Arbeitsplatz (***Offline-Arbeitsplatz***) bearbeitet. Die Daten befinden sich niemals auf den Festplatten der PC, sondern immer auf separaten, externen Datenträgern (***Datenbasis***).



Es muss heute von der Vermutung ausgegangen werden, dass auf herkömmliche Weise betriebene PC prinzipiell nicht ausreichend gegen Angriffe aus dem Internet abgesichert werden können. Wird - wie üblich - die Software eines Personalcomputers auf der Festplatte installiert, so kann diese Software jederzeit verändert werden. Das bedeutet aber eben auch, dass die Software jederzeit durch Schadprogramme (Viren, Trojaner usw.) oder Angriffe von außen dauerhaft (persistent) manipuliert und damit korrumpiert werden kann. Fast alle ernsten und erfolgreichen Angriffe aus dem Internet beruhen auf solchen persistenten Manipulation von Software auf dem PC.

Mit einem auf Festplatte installierten Betriebssystem wie beispielsweise MS-Windows kann deshalb jeder Computer aus Sicherheitsgründen nur eine Rolle - also ***entweder*** Online- ***oder*** Offline-Arbeitsplatz - übernehmen. Es wird also je ein PC für jeden Arbeitsplatz benötigt, wobei der im Online-Arbeitsplatz verwendete Personalcomputer trotz aller herkömmlichen Sicherheitsmaßnahmen letztlich ein „Opferrechner" (BSI) ist:



Befindet sich die Software des Computers dagegen auf einer CD (einer sog. Live-CD) und wird die Software von dieser CD gestartet, dann sind solche persistenten Manipulationen ***physikalisch*** bedingt unmöglich. Damit werden aber auch ***alle*** gegen solche persistenten Manipulationen gerichteten herkömmlichen Absicherungen wie etwa Virenscanner überflüssig. Allein dies reduziert sowohl die Komplexität der Softwarenutzung am PC als auch den Zeitaufwand für sekundäre, nicht mit der eigentlichen Arbeit des PC-Nutzers zusammenhängende Tätigkeiten am Computer dramatisch.

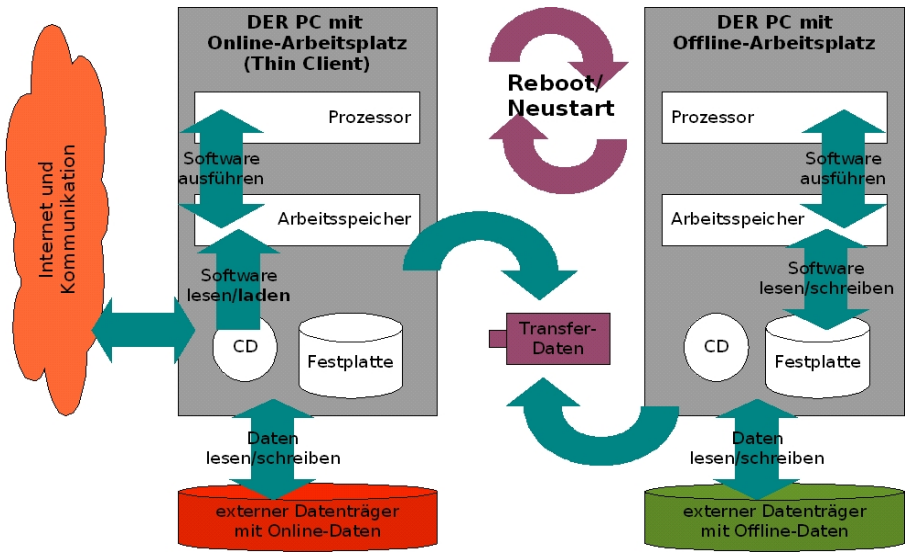
Die Live-CD ist dabei kein Ersatz für ein vollständiges, auf der Festplatte installiertes Betriebssystem (MS-Windows, Mac-OS, Linux). Eine Live-CD ist vielmehr eine Ergänzung für das installierte Betriebssystem:

- als sicherer Internetzugang (Online-Arbeitsplatz);
- als sicheres Werkzeug zur Datenbearbeitung und Datenverwaltung (Offline-Arbeitsplatz);
- bei Bedarf als sicherer und zuverlässiger Virenscanner.

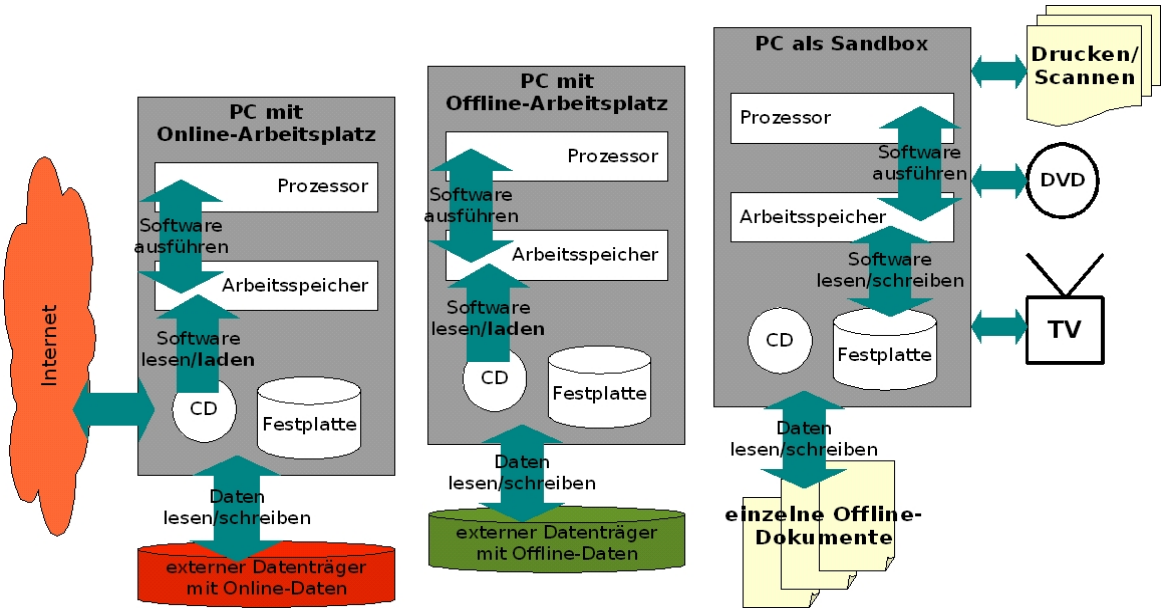
Jede Live-CD verwendet ein eigenes Betriebssystem (in der Regel Linux), um den Computer unabhängig von MS-Windows zu starten. Dieses eigene Betriebssystem kann aber für den PC-Nutzer auch transparent gestaltet werden. Der Nutzer sieht dann eine Live-CD nicht als ein - mühsam neu zu erlernendes - Betriebssystem, sondern einfach als eine Sammlung von - gut bekannten – Anwendungsprogrammen:

- Die Live-CD als Internetbrowser *Firefox*, wie er ihn auch unter MS-Windows kennt.
- Die Live-CD als Dateimanager *Konqueror* (KDE), der ähnlich wie der *Windows-Explorer* bedient werden kann.
- Die Live-CD als *Open Office*, das genau wie unter MS-Windows funktioniert (vielleicht ein paar andere Schrifttypen).

Der Neustart (Booten) einer Live-CD erzielt den gleichen Effekt wie die physikalische Trennung zweier Rechner, weil die Software des Rechners von einem nicht-manipulierbaren Medium praktisch völlig neu aufgebaut wird. Die laufende Software einer Live-CD kann dabei nicht durch Schadsoftware beeinflusst werden, die vorher auf der Festplatte oder im Arbeitsspeicher des Rechners installiert wurde (evtl. Ausnahme: BIOS). Mit einer Live-CD kann dabei ***jeder Computer jede Rolle*** und ***ein Computer abwechselnd beide Rollen*** übernehmen. Online- und Offline-Arbeitsplatz können so auch mit einem einzelnen PC realisiert werden:



Ich empfehle, sowohl den Online- als auch den Offline-Arbeitsplatz mit Live-CD und einen externen Datenträger (USB-Stick) betreiben:



Die Nutzung der Live-CD im Online-Arbeitsplatz ist aus Sicherheitsgründen zwingend. Im Offline-Arbeitsplatz verhindern Live-CD und externer Datenträger, dass - unbemerkt vom Nutzer - Fragmente vertraulicher Daten auf der Festplatte abgelegt werden. Das auf der Festplatte installierte Betriebssystem, also meist MS-Windows, wird als „Sandbox" betrieben, es ist nach außen vollständig isoliert. Diese Sandbox dient zur Bearbeitung komplexer Offline-Dokumente, die mit einer Live-CD nur umständlich zu bearbeiten wären, außerdem zur Nutzung von Peripheriegeräten (Treiber) und zu Unterhaltungszwecken.

Der Betrieb eines Personalcomputers mit einer Live-CD ist nach dem heutigen Stand der Technik der sicherste Schutz gegen Angriffe und Manipulationen. Deshalb kann bei bürotypischer Nutzung in der Regel der Online-Arbeitsplatz als Standardarbeitsplatz benutzt werden, auf dem durchaus auch einzelne vertrauliche Dokumente zeitweise/teilweise bearbeitet werden. Die Existenz eines isolierten Offline-Arbeitsplatzes dient vor allem der Sicherung des ***Gesamtdatenbestands***. Damit und durch eine entsprechende Organisation der Daten kann der Einsatz einer Live-CD - der ja auf den ersten Blick recht umständlich erscheint - in den Alltag eines normalen PC-Arbeitsplatzes integriert werden, ohne die eigentliche Arbeit des PC-Nutzers durch komplizierte und zeitraubende Prozeduren zu behindern.