

Die Sicherheit Ihres Praxisverwaltungssystems

Was Sie im Umgang mit EDV-Anlagen und Onlinediensten beachten sollten

Gefahren bei Sicherheitslücken

Ihr Praxisbetrieb ist in hohem Maße abhängig von Ihrem EDV-System, Ausfallzeiten ziehen einen hohen potentiellen Schaden nach sich.

Über folgende Risiken sollten Sie sich bewusst sein:

- Datenverlust durch defekte Hardware, Zerstörung, Manipulation oder Diebstahl
- Datenunsicherheit durch unerlaubten Zugriff auf sensible Patienten- und Behandlungsdaten

Diese Risiken können erhebliche rechtliche und finanzielle Konsequenzen haben.

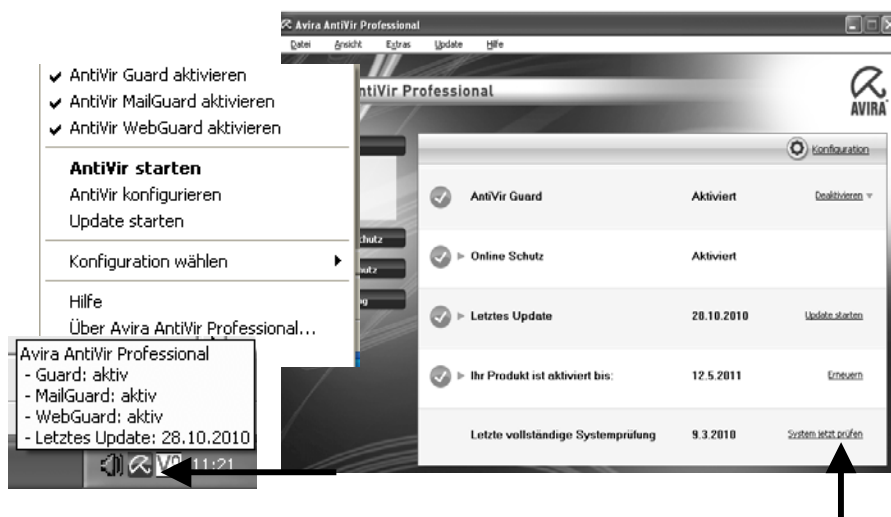
Sie können sich davor schützen! Wenn Sie folgende Maßnahmen konsequent beachten, können Sie ohne hohen Aufwand und ohne die Notwendigkeit von speziellen Vorkenntnissen die Basissicherheit Ihres Computersystems gewährleisten.

Schutz vor Viren

Viren löschen Dateien oder beschädigen Ihr Betriebssystem. Oftmals fällt der Rechner ganz aus, weil Sie keinen Zugriff mehr auf Ihre Dateien haben. Die Übertragung findet über den Download aus dem Internet oder über Wechselmedien (USB-Stick, CDs, Disketten) statt.

Als Schutz sollten Sie ein Virenschutzprogramm installieren. Verschiedene Firmen bieten im Internet vom Basisschutz bis zum Rundumschutz leistungsfähige Programme an. Aber damit ist es nicht getan! Da täglich neue Virenarten entstehen können, ist die laufende Aktualisierung der Erkennungsdateien für Viren unerlässlich. Viele Programme erleichtern Ihnen das durch automatische Updates.

Im nebenstehenden Beispiel wird das Vorgehen mittels des Avira Virenschanners erläutert. Auf dem Markt gibt es weitere kostenfreie oder kostenpflichtige Virenschanner, wie z. B. Avast, Norton Security, Kasperski, McAfee und viele andere mehr, die gleichwertig verwendet werden können.



Sollten Ihre Programme auffällig reagieren, kann ein Virenbefall vorliegen. Dann können Sie über die abgebildete Konsole – hier am Beispiel AntiVir – des Virenschanners einen Systemscan starten, um verborgene Schädlinge aufzuspüren.

Schutz vor Datenverlust

Festplatten und Wechseldatenträger haben nur eine begrenzte Lebensdauer. Auch äußere Einflüsse können die Hardware zerstören, so dass ein Datenverlust unvermeidlich ist, wenn Sie nicht für regelmäßige Sicherungen gesorgt haben. Kopieren Sie daher wichtige Dateien auf CDs, besser noch wegen ihrer längeren Lebensdauer auf externe Festplatten. Diese haben weit mehr Kapazität und können zu erschwinglichen Preisen mit hoher Speicherkapazität erstanden werden. Um eine vollständige Sicherheit zu erzielen, transportieren Sie die kopierten Daten in regelmäßigen Abständen aus Ihrer Praxis an einen anderen Ort, zum Beispiel Ihr zuhause. So ist auch im Brandfall gewährleistet, dass Ihre Daten nicht verloren gehen können.

Schutz vor Sicherheitslücken

Betriebssysteme und Programme werden laufend optimiert und zur Abwehr neuartiger Sicherheitsrisiken angepasst. Daher sollten Sie Sicherheitsupdates (Patches) regelmäßig automatisch oder, wenn das nicht möglich ist, manuell durchführen. Damit bleibt Ihre Software auf dem neuesten Stand!

Ihr Windows-Betriebssystem lässt sich so konfigurieren, dass Updates automatisch durchgeführt werden. Dies ist auch in der Regel bei Ihrer Anwendungssoftware so. Natürlich können Sie immer wieder manuell prüfen, ob neue Updates im Internet vorliegen und so Ihre Sicherheitseinstellungen gezielt kontrollieren.

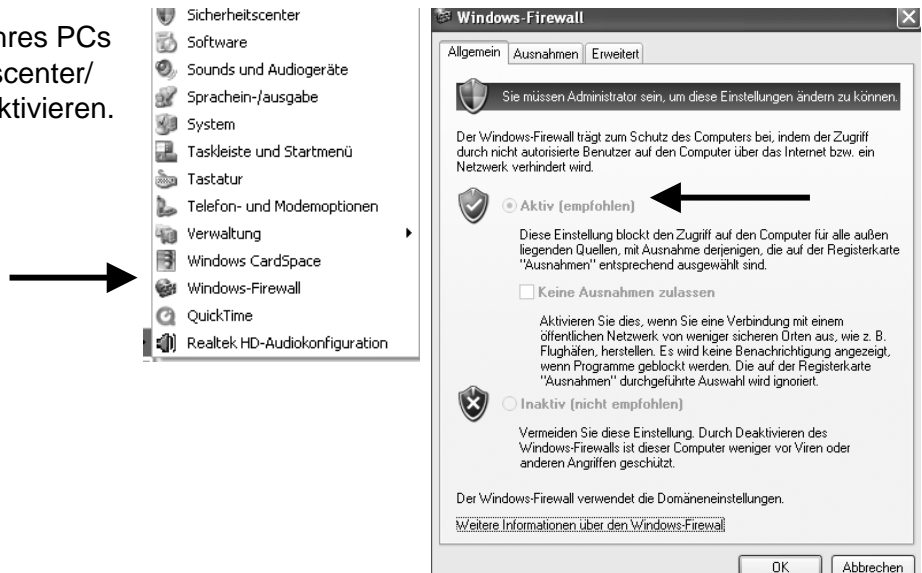
The image shows a Windows XP desktop environment. On the left, the Start menu is open, and the 'Systemsteuerung' (Control Panel) icon is highlighted. Below it, the 'Automatische Updates' (Automatic Updates) window is open, showing the 'Schützen Sie den Computer' (Protect your computer) section. The 'Automatisch (empfohlen)' (Automatic (recommended)) option is selected, and the settings are configured to download updates daily at 12:00. On the right, the 'Windows-Sicherheitscenter' (Windows Security Center) window is open, displaying the 'Wesentliche Sicherheitsmaßnahmen' (Essential security actions) section. The 'Automatische Updates' (Automatic Updates) link is highlighted with a black arrow. A black arrow also points from the 'Sicherheitscenter' icon in the Start menu to the Security Center window. Another black arrow points from the 'Automatische Updates' link in the Security Center window to the 'Automatische Updates' window.

In der Systemsteuerung Ihres PCs können Sie im Sicherheitscenter/Automatische Updates den automatischen Download und Installation der Patches einstellen.

Schutz vor Angriffen aus dem Internet

Ungeschützte Computersysteme, die eine Verbindung zum Internet haben, können Angriffen aus dem Netz ausgesetzt sein. Zum Beispiel nisten sich sogenannte Trojaner in Ihr Betriebssystem ein und können sensible Informationen an den Urheber dieser Schadsoftware zurücksenden. Dagegen hilft eine Firewall. Im Windowsbetriebssystem ist eine Basisfirewall bereits enthalten und muss aktiviert sein. Kommerzielle Personal-Firewalls bieten mitunter einen Rundumschutz.

In der Systemsteuerung Ihres PCs können Sie im Sicherheitscenter/Windows-Firewall diese aktivieren.



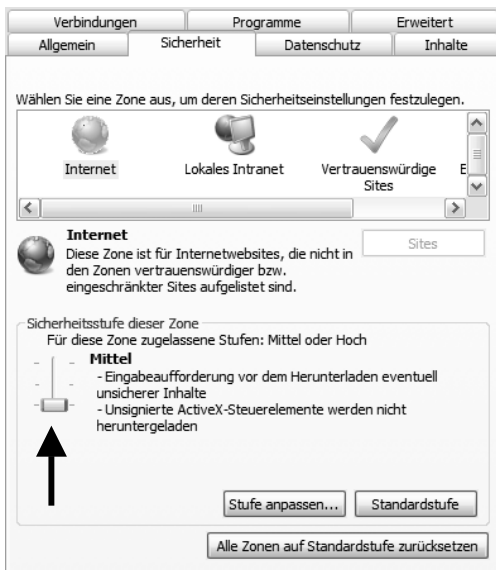
Schutz vor ungewolltem Login

Kennwörter bilden einen sicheren Schutz vor ungewollten Zugriffen am Rechner selbst und über Netzverbindungen. Vermeiden Sie daher Passwörter aus persönlichen Daten (Geburtsdatum, Reisevorlieben etc.) oder Eigennamen aus Ihrem Umfeld. Besser sind Kombinationen aus Buchstaben und Zahlen. Kennwörter sollten in regelmäßigen Abständen geändert werden und niemals im PC oder auf Papier gespeichert oder notiert werden.

Schutz vor Browserlücken

Webbrowsern, wie Internetexplorer oder Firefox sollten Sie nicht erlauben, persönliche Daten zu speichern. Diese Möglichkeit wird dort oft angeboten, um Anmeldeprozesse zu vereinfachen. Ihr PC speichert diese Information als „Cookie“ ab, daher suchen Hacker bei unerlaubten Angriffen gerne danach. Erhöhen Sie bei Bedarf die Sicherheitseinstellungen in Ihrem Webbrowser und Ihres Mailprogramms.

Microsoft Internetexplorer: Einstellen der Sicherheitsstufe mit Schieberegler



Im Internetexplorer können Sie unter Extras/ Internetoptionen die Sicherheitsstufe anpassen. Von Zeit zu Zeit empfiehlt es sich auch, Verlauf und Cookies zu löschen.

Mozilla Firefox: Einstellungen zur Sicherheit

Mozilla Firefox bietet eine ähnliche Funktion unter Extras/Einstellungen/Sicherheit. Hier können Sie auswählen, welche Optionen aktiviert sein sollen. Bei der Speicherung von Passwörtern empfiehlt es sich beispielsweise, das Häkchen zu entfernen. Unter Erweitert/Netzwerk können Sie alle gespeicherten Verlaufdaten im sogenannten Cache löschen.

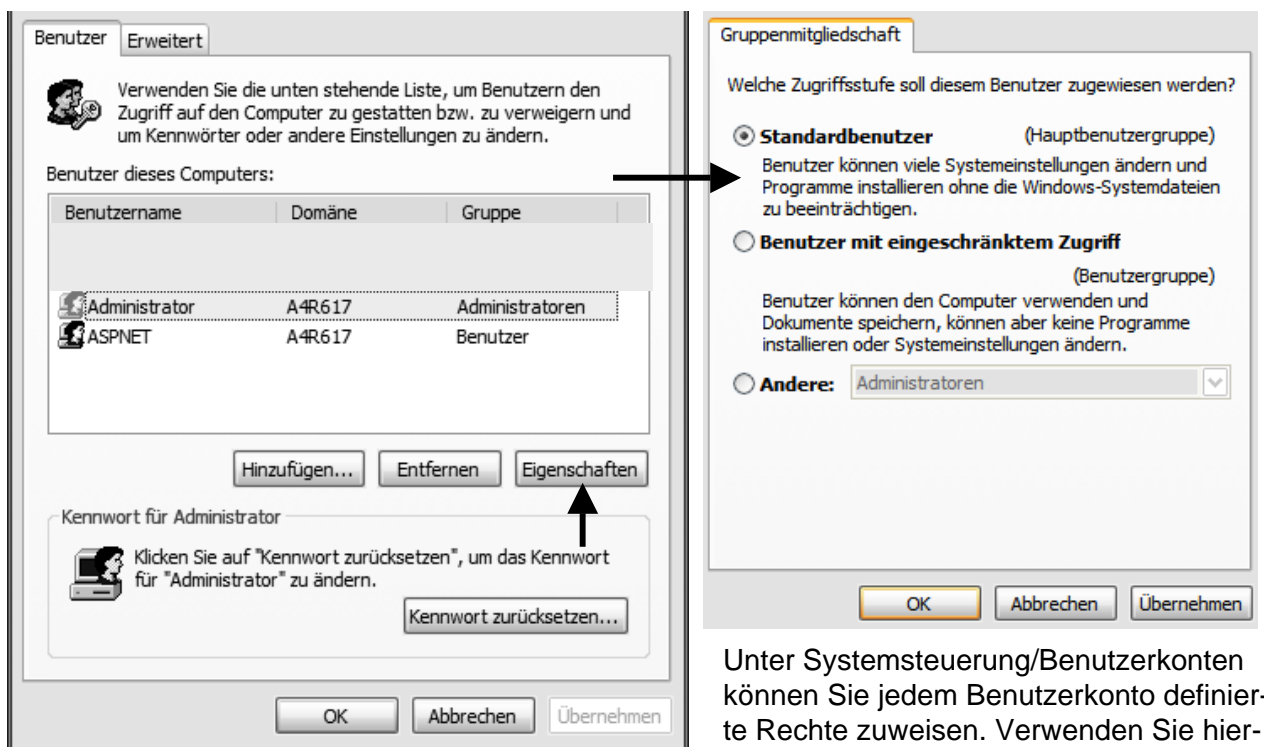


Schutz vor Datenklau

Stellen Sie den PC nicht so auf, dass er längere Zeit unbeobachtet ist. Datenklau und Datenmanipulation kann auch am Rechner selbst vorgenommen werden. Sichern Sie den Zugang zum Computer, indem er bei Ihrer Abwesenheit nicht einfach zugänglich ist.

Schutz durch Benutzerrechte

Nicht jeder Ihres Praxisteam sollte auf alle Daten zugreifen oder Löschmöglichkeiten haben. Die Benutzerverwaltung unter Windows bietet zahlreiche Möglichkeiten, Benutzerrechte festzulegen. Zum Beispiel haben Benutzer mit eingeschränktem Zugriff keine Möglichkeit, Programme zu installieren, Systemänderungen vorzunehmen oder ungewollt auf Daten zuzugreifen. Als Praxisleiter sollten Sie als Einziger Administratorenrechte ausüben dürfen.



Unter Systemsteuerung/Benutzerkonten können Sie jedem Benutzerkonto definierte Rechte zuweisen. Verwenden Sie hierfür den Knopf „Eigenschaften“

Schutz durch klare Arbeitsanweisungen

Machen Sie Ihrem Praxisteam klare Vorgaben zum Umgang mit dem Internet. Private Downloads und privates Surfen, sowie Postabrufe über private Mailprogramme sollten unterbleiben. Mails unbekannter Herkunft mit Anhang sollten niemals geöffnet werden, da sich dahinter einen Virenangriff verbergen könnte. Löschen Sie daher am besten diese Mails.

Rundum sicher

Das EDV-System Ihrer Praxis ist ein unverzichtbares Instrument Ihrer Praxisverwaltung. Wenn Sie die oben genannten Grundregeln anwenden, schaffen Sie eine solide Basis zum sicheren Umgang mit Ihrem Praxissystem und den Daten ihrer Patientinnen und Patienten.