Sicherer Arbeitsplatz

RED Medical verwendet starke Verschlüsselung, um Ihre sensiblen Daten zu jedem Zeitpunkt vor dem Zugriff Unbefugter zu schützen. Auf Ihrem Arbeitsplatz, dem Rechner, Tablet oder Mobiltelefon, das Sie zur Arbeit mit RED Medical verwenden, müssen die Daten im Klartext vorhanden sein, damit Sie mit diesen arbeiten können. Daher sollten Sie darauf achten, dass Sie Ihren Rechner zusätzlich schützen.

Hinweise des Bundesamtes zur Sicherheit in der Informationstechnik für Passwörter

Hinweise zu Passwörtern von Deutschland-sicher-im-Netz e.V.

Sichere Anmeldung und Sperre

Ein unbeaufsichtigter Arbeitsplatz, an dem ein Benutzer eingeloggt ist, stellt ein großes Sicherheitsrisiko dar, wenn unberechtigte Personen Zugang zu diesem erhalten können. Bitte beachten Sie daher folgende einfache Sicherheitsmaßnahmen:

- Beim Eingeben Ihres Passwortes darf Ihnen niemand zusehen.
- Beim Verlassen des Arbeitsplatzes sollten Sie sich entweder aus dem System ausloggen oder den Zugriff sperren.
- RED Medical verfügt darüberhinaus über einen automatischen Mechanismus, der einen Benutzer nach 10 Minuten der Inaktivität automatisch ausloggt. So wird verhindert, dass nach dem Verlassen eines Arbeitsplatzes weiterhin Zugriff besteht.

Passwörter

Sie sollten für die Anmeldung in RED möglichst sichere Passwörter verwenden. Dazu beachten Sie bitte folgende Hinweise:

- Geben Sie ihr Passwort niemals an eine andere Person weiter.
- Wenn Sie Ihr Passwort aufschreiben, verwahren Sie es an einem für Dritte unzugänglichen Ort und vermerken Sie nicht zu welchem System das Passwort gehört. Besser ist, das aufgeschriebene Passwort etwas zu verändern.
- Passwörter müssen mit einer hinreichenden Stärke eingegebenen werden - grundsätzlich gilt, dass ein Passwort umso sicherer ist, je länger es ist. Daher macht RED es Ihnen zur Auflage, dass Ihr Passwort aus mindestens 10 Zeichen besteht.
- Als Passwörter sollten keine "normalen" Wörter verwendet werden, die Sie in einem Wörterbuch finden können (z.B. "Passwort", "Demo", "Admin"). Hacker verwenden Listen solcher bekannter Wörter, um Passworte zu erraten.
- Als zusätzlichen Sicherheitsmechanismus verlangt RED Medical, dass Sie Ihr Passwort alle 90 Tage ändern.

Erlkönig - Passwortänderung

RED connect - Administration

Arbeitsplatz-Freischaltung

In RED Medical können Sie nur Arbeitsplätze verwenden, die extra freigeschaltet wurden. Damit wird verhindert, dass Unbefugte selbst bei Kenntnis gültiger Zugangsdaten von außen auf Ihre Daten zugreifen können. Diese Freigabe kann auch zeitweilig erfolgen (z.B. für einen Heim-PC einer Mitarbeiterin, die die Privatliquidation über das Wochenende von zuhause erledigt) und jederzeit widerrufen werden. Insbesondere die temporäre Abmeldung kann und sollte im Rahmen von Urlaubszeiten für Heimarbeitsplätze, Laptops und andere mobile Geräte, die sich im Zugriff des im Urlaub befindlichen Mitarbeiters befinden, genutzt werden.

Erlkönig - Arbeitsplatz freischalten

RED connect - Administration

Firewall

Zu beachten ist auch, dass bei einem mit dem Internet verbundenen System ein Zugang auch von außen über Methoden des “Hackings” vorgenommen werden kann. Ein solches System muss daher mit entsprechenden Schutzmaßnahmen ausgestattet sein. Wir empfehlen dringend, sowohl das Netzwerk (Router-Firewall) als auch jeden einzelnen Arbeitsplatz (Personal-Firewall) mit einer entsprechenden Firewall-Software auszustatten.

Virenscanner

Darüber hinaus sollte auf jeden Arbeitsplatz eine aktuelle Virensoftware installiert sein, die über einen eingebauten Updatemechanismus idealerweise täglich (oder noch öfter) die entsprechenden Virensignaturen und Erkennungsalgorithmen aktualisiert.

Weitergehende Internet-Nutzung

Beim Aufruf von Webseiten unbekannter Herkunft setzt sich jeder Internetnutzer der Gefahr aus, ungewollt Schadsoftware auf seinem Arbeitsplatz zu installieren. Diese Gefahr kann zwar durch den Einsatz eines Virenscanners (s.o.) minimiert werden, ganz ausgeschlossen werden kann sie aber nicht. Aus diesem Grund empfehlen wir auf den für RED Medical genutzten Arbeitsplätzen den Aufruf anderer Internet-Seiten möglichst zu vermeiden. Zumindest sollte dieser aber auf Webseiten begrenzt werden, die dem Anwender gut bekannt sind und die der Förderung der Systemsicherheit dienen (z. B. Herstellerseiten, um auf Updates zu prüfen). Gegebenenfalls kann auch eine Software, die normalerweise zur Kindersicherung eingesetzt wird, dazu verwendet werden, um die Internetnutzung auf den Arbeitsplätzen entsprechend einzuschränken.

Sonstige Software

Wir empfehlen auf den Einsatz sonstiger Software, die nicht direkt für die ärztliche Tätigkeit benötigt wird (wie z. B. die Steuersoftware eines medizinisch-technischen Gerätes), zu verzichten. Das betrifft auch und insbesondere Software, die selbst eine Verbindung zum Internet aufnehmen. Beispielhaft seien hier private Spiele genannt. Ganz grundsätzlich sollte bei der Nutzung eines jeden Programmes auf einem der RED Medical-Arbeitsplätze sorgfältig abgewogen werden, ob dessen Verwendung unbedingt notwendig ist.

Updates

Wir empfehlen dringend, in regelmäßigen Abständen (mindestens einmal pro Woche) die entsprechenden Update-Suchfunktionen oder Informations-Seiten des Betriebssystem-Herstellers sowie der Hersteller der sonstigen auf den Arbeitsplätzen genutzten Software (insbesondere des Browsers, aber auch Office o.ä.) daraufhin zu überprüfen, ob neue, sicherheitsrelevante Updates vorliegen. Wir empfehlen, diese zunächst auf einem Testrechner einzuspielen und sich in angemessener Weise davon zu überzeugen, dass alle systemkritischen Programmteile einwandfrei funktionieren. Erst dann sollten die Updates auf allen anderen Arbeitsplätzen eingespielt werden.

Die meisten Betriebssysteme, Browser und auch sonstige Software verfügen inzwischen über eine sog. "Auto-Update"-Funktionalität. Diese hat den Vorteil, dass die vorgenannten Überprüfungen auf Aktualisierungen von der Software selbst und automatisch vorgenommen werden. Sie haben aber auch den Nachteil, dass Updates sich u. U. zu zeitlich unpassenden Terminen aktivieren und dabei möglicherweise sogar einen Reboot des Rechners erfordern. Darüber hinaus besteht die Gefahr, dass systemkritische Programmteile nach dem Update nicht mehr funktionieren. Aus diesem Grund empfehlen wir den Einsatz einer Auto-Update-Funktion nur dann, wenn sich dieser zunächst nur auf den Hinweis, dass ein Update vorliegt, beschränkt und der eigentliche Update-Vorgang manuell vom Anwender aktiviert werden muss. Auf diese Weise kann man die Vorteile der Funktion nutzen und die Nachteile weitestgehend eliminieren.