HINWEISE ZU INTERNETSICHERHEIT, VIRENSCANNER UND FIREWALL FÜR DS-WIN

Version: 2.3

Pionier der Zahnarzt-Software.
Seit 1986.

DAMPSOFT
Die Zahnarzt-Software

1. Internetsicherheit

In diesem Dokument möchten wir Ihnen Hinweise für die Konfiguration Ihres Virenscanners und Ihrer restriktiv eingerichteten Firewall geben. Es richtet sich an Administratoren, Systembetreuer oder Verwalter des Virenscanners bzw. der Firewall.

Falls Sie einen Virenscanner oder eine Firewall in der Praxis verwenden, mit deren Konfiguration aber nicht vertraut sind, wenden Sie sich bitte mit diesem Dokument an Ihr betreuendes Systemhaus. Der Dampsoft-Kundenservice sowie der Technische Support kann und wird Fragen zur Konfiguration Ihrer IT-Sicherheitsumgebung nicht beantworten, da es sich dabei um einen Teil des Praxisnetzwerks handelt, den ausschließlich Ihr Systemadministrator konfigurieren sollte.

1.1. Allgemeine Hinweise zur Internetsicherheit

Bitte beachten Sie grundsätzlich, dass eine unsachgemäße Konfiguration Ihres Virenscanners oder Ihrer Firewall zu erheblichen Sicherheitslücken oder Internetverbindungsproblemen führen kann. Das Freigeben von Verbindungen ins Internet birgt grundsätzlich und naturgemäß ein Sicherheitsrisiko und sollte daher nur nach eingehender Analyse der möglichen Risiken durch den Systemadministrator geschehen. Die unten folgenden Einstellungsvorschläge dürfen nur als Empfehlung verstanden werden. Um die Risiken zu reduzieren, sollten Sie nur genau die Ausnahmen einstellen bzw. Verbindungen zulassen, die Sie zwingend benötigen.

Bitte beachten Sie weiter, dass Virenscanner und Firewall nur Teile eines umfassenden Sicherheitskonzepts in Ihrer Praxis sind. Neben ihnen sind unter anderem aktuelle Updates für Betriebssystem, Browser und alle anderen im Internet verwendeten Programme absolute Pflicht! Die meisten Fälle von Virenbefall lassen sich auch durch den achtsamen Umgang mit Emails und USB-Speichersticks verhindern. Die Erstellung eines Sicherheitskonzeptes, das auf die individuellen Bedürfnisse Ihrer Praxis zugeschnitten ist, ist Aufgabe Ihres Systembetreuers. Dampsoft kann diese Beratung und Einrichtung nicht übernehmen. Das gilt auch für eine eventuelle Haftung im Schadensfall.

2.1. Allgemeines zum Virenscanner

Die Hintergrundaktivitäten des Virenscanners können in Abhängigkeit zur Leistungsfähigkeit des Computers und des Netzwerks oder zum DS-Win-Datenvolumen negative Auswirkungen auf die Programmperformance haben. In seltenen Fällen kommt es auch zu Fehlalarmen, sogenannten „false positives“, bei denen die Automatik des Virenscanners fälschlich eine Infektion annimmt. Diese Nebeneffekte lassen sich niemals hundertprozentig ausschließen. Sie können aber durch die Konfiguration der Überwachungsausnahmen deutlich reduziert werden.

Virenscanner verwenden in der Regel zwei Mechanismen, die bei jedem Hersteller individuell bezeichnet werden:

- der "Dateiscan" prüft Dateien und Verzeichnisse, wenn darauf zugegriffen wird oder wenn ein geplanter Prüflauf durchgeführt wird
- die "Prozessüberwachung" überwacht das Verhalten von ausgeführten Programmen

Bitte beachten Sie, dass die hier vorgeschlagenen Änderungen ausschließlich Dampsoft-Programme betreffen. Für verwendete Drittsoftware (z.B. Röntgenprogramme) erhalten Sie entsprechende Empfehlungen vom jeweiligen Hersteller.

2.2. Dampsoft empfiehlt folgende Ausnahmen für den Virenscanner

Für den Dateiscan und die „Echtzeitüberwachung von Dateien“:

Modul / Dienst	Empfohlene Ausnahmen
DS-Win-Datenbankdateien	Dateien mit den Endungen *.cdx, *.dbf, *.lck, *.tim und *.fpt im Verzeichnis <Lw>:\TDAMP\DS\ und <Lw>:\TDAMP\TMX\ sowie allen Unterverzeichnissen
DS-Win-Fingerabdruckdatenbank (bei Verwendung eines Fingerscanners mit DS-Win)	<Lw>:\TDAMP\DS\DATEN\DSWINDB.DSF

Für die Prozessüberwachung:

Modul / Dienst	Empfohlene Ausnahmen
DS-Win-Hauptprogramm	DSWIN.EXE DSPRG.EXE
DS-Win-Termin	TERMINIX.EXE
DS-Win-View	DSVIEW.EXE
DS-Win-Fibu	FIBU.EXE
DS-Win-BuS	DSSTERIS.EXE DSSIEGEL.EXE
DS-Win-Zeit	DSZEIT.EXE
Athena	DSSERVER.EXE HTTPD.EXE
Anbindung für Sirona Sidexis XG	DSSIDEX.EXE

Modul / Dienst	Empfohlene Ausnahmen
Anbindung für VDDS-Röntgenprogramme	DSPATIMP.EXE DSPICEXP.EXE DSPICIMP.EXE DSPICPUT.EXE DSPICVJU.EXE

2.3. Weitere Hinweise

Zu Testzwecken kann auch der gesamte TDAMP-Ordner vom Echtzeit-Viren-Scan ausgeschlossen werden. Da dabei eine unnötig große Sicherheitslücke geöffnet wird, ist dieses Vorgehen für den Dauerbetrieb nicht empfohlen! Bei Nutzung des Dampsoft-E-Mail-Clients bedeutet dies beispielsweise, dass die dort abgelegten E-Mail-Dateien keinem Virenschutz unterliegen. Achten Sie deshalb bitte unbedingt darauf, den Virenschutz nach dem Test wieder korrekt zu konfigurieren.

Um die in Punkt 2.2. ausgeschlossenen Dateien dennoch nicht gänzlich ungeschützt zu belassen, sollten sie regelmäßig einem Komplett-Scan unterzogen werden, der ohne die o.g. Ausschlüsse durchgeführt wird.

2.4. Erfahrungen/Troubleshooting

Falls Sie trotz korrekter Konfiguration des Virenscanners Einschränkungen bei der Performance der Dampsoft-Programme feststellen, deinstallieren Sie den Virenscanner bitte testweise von allen beteiligten Systemen. Nur so lassen sich die Hintergrundprogramme als mögliche Ursache sicher ausschließen, da sie beim einfachen „deaktivieren“ teilweise weiter aktiv sind.

Bitte beachten Sie, dass es in einigen Konfigurationen auch möglich ist, dass DS-Win indirekt durch angebundene Drittprogramme (z.B. Röntgensoftware) ausgebremst werden kann, wenn diese durch den Virenscanner verzögert auf Anfragen reagieren.

3.1. Allgemeines zur Firewall

DS-Win benötigt im Regelfall im lokalen Netzwerk nur die Windows-Dateifreigabedienste. Für bestimmte Module werden zusätzliche Verbindungen ins Internet benötigt. Eine sichere Firewall würde diese Verbindungen blockieren und damit die Programmfunktionen einschränken.

In diesem Abschnitt möchten wir Ihnen für die Konfiguration Ihrer restriktiv eingerichteten Firewall die Verbindungen mitteilen, die für die Online- und Netzwerk-Dienste von Dampsoft genutzt werden.

Bitte beachten Sie, dass die Verwaltung der Firewall in der Praxis eigenverantwortlich geregelt wird. Sicherheitslücken im Browser oder dessen Erweiterungen sowie auch der unsachgemäße Umgang mit dem Internet (insbesondere Emails) können trotz Firewall zu Schäden bzw. Fremdzugriffen führen. Daher garantiert auch eine restriktive Firewall allein keine absolute Sicherheit.

Für die Anbindung einiger netzwerkfähiger Geräte in Ihrer Praxis sind evtl. weitere Einstellungen notwendig. Da diese in Bezug auf IP-Adressen, Netzwerknamen und Verbindungsanschlüsse (Ports) individuell eingestellt werden, können wir dazu keine allgemein gültigen Hinweise geben. Über das Netzwerk lassen sich neben Softwareprodukten auch einige Geräte anbinden. Dazu gehören beispielsweise:

- Kartenleser für die elektronische Gesundheitskarte (eGK)
- Sterilisatoren
- Siegelgeräte

Falls bei diesen Geräten keine Kommunikation mit dem PC möglich ist, prüfen Sie bitte neben den Einstellungen der Anbindung auch die Firewall.

3.2. Online-Dienste

Im Folgenden listen wir die Dampsoft-Dienste und deren notwendige Verbindungen auf. Die genannten IP-Adressen können sich jederzeit ändern, z.B. wenn wir Dienste umstellen, um die optimale Funktion sicherzustellen. Diese Liste muss dabei nicht zwingend aktualisiert werden. Wir empfehlen daher die Verwendung der aufgeführten URLs. Dabei wird eine korrekte Namensauflösung vorausgesetzt.

3.2.1. Eingehende Verbindungen:

Modul / Dienst	Notwendige Verbindungen
DS-Win-Net	- Port 443 und 4044 (TCP) auf den Terminbuch-Server in der Praxis
DSServer (Athena)	- Port 24351 (TCP), Remoteport „Alle Ports“ auf DSServer-Rechner
Controlling Cockpit	- Port 24352 (TCP) während der Aktivierung

3.2.2. Ausgehende Verbindungen:

Modul / Dienst	Notwendige Verbindungen
Allgemein für jede Web-Schnittstelle (z.B. DS-Win-Comm, SMS-Cockpit, OTM, Controlling-Cockpit, …)	- Port 443 (TCP) auf api.dampsoft.de (153.92.34.59)
DS-Win-Comm und SMS-Versand	- Port 443 (TCP) auf dswincomm.dampsoft.de (80.149.230.116)
Online-Terminmanagement	- Verbindung DS-Win-Comm - Port 443 (TCP) auf *.termin.dampsoft.net
Smartphone-Anbindung	- Verbindung DS-Win-Comm (siehe oben) - Port 443 (TCP) auf kalender.dampsoft.de (180.40.16.54)
Internet-Update laden	- Port 80 (TCP) auf api.dampsoft.de (153.92.34.59) - Port 21 und ggf. 20 (TCP) auf download.dampsoft.de (78.47.28.1, 188.40.249.145)
Laborpreise herunterladen	- Port 80 (TCP) auf api.dampsoft.de (153.92.34.59)
DS-Win-Remote 2	- Es handelt sich um eine Remote-Verbindung über Teamviewer. Eine konkrete Angabe der verwendeten IP-Adressen ist aufgrund der Anzahl der Server nicht möglich. Es sollte ausreichen, wenn einer der folgenden Ports zum Internet offen ist: 80, 443 oder 5938 (TCP).
DS-Win-E-Mail-Client	- Die für die Verbindung notwendigen Internetadressen und Ports für den Posteingangs- und –ausgangsserver erfragen Sie bitte bei Ihrem E-Mail-Anbieter.
Athena Dashboard & Anamnese@Home	- Port 443 (TCP) auf https://dashboard.athenaapp.de (54.171.32.62) - DNS-Rebind-Schutz deaktivieren für *athenabox.de* - Port 443 (TCP) auf https//anamnese.athenaapp.de und https://anamnese-at-home-backend.athenaapp.de/
Rise KIM-Client-Modul	- Port 443 (TCP) auf https://am.kimplus.de [Account-Manager für Registrierung/Verwaltung von KIM-Adressen] - Port 443 (TCP) auf https://obs.rise-kim.de [RISE-OnBoarding-Service für Registrierung von KIM-Adressen] - Port 80 (TCP) auf http://status.geotrust.com [OCSP-Rsponder für Prüfung des Zertifikates vom Account-Manager]
KIM-Client-Modul anderer Anbieter	Zur Registrierung und Verwaltung von KIM-Adressen sind in der Regel ausgehende Verbindungen nötig. Bitte entnehmen Sie die nötigen Firewall-Einstellungen der Dokumentation des Anbieters. Allgemeingültige Hinweise zur Installation finden Sie in unserer KIM-Installationsanleitung auf www.dampsoft.de im Bereich „Service – Infos für Systembetreuer“.

* bitte Hinweise für „ausgehende Verbindungen“ auf der Folgeseite beachten

Hinweise für „ausgehende Verbindungen“:

In einigen Fällen werden dynamische IP-Adressen genutzt. Sollte dazu die aktuelle IP-Adresse erforderlich sein, so empfehlen wir zum Beispiel über die CMD-Konsole den „NSLOOKUP-Befehl“ zu nutzen, um die IP-Adresse aufzulösen (nslookup kalender.dampsoft.de).

Falls Sie besondere Internet-Security-Lösungen (z.B. Sophos, SecurePoint,…) einsetzen, sollten Sie bei der Einrichtung berücksichtigen, dass „ausgehende Verbindungen“ dort möglicherweise auch Regeln für die entsprechenden Antwortpakete der oben angegebenen Domainnamen erfordern können.
Dies sollte aus der Dokumentation zu den Geräten/ Lösungen hervor gehen.

3.3. Lokale Dienste

Dampsoft-Dienste, die in der Regel ausschließlich im lokalen Netzwerk betrieben werden:

3.3.1. Eingehende Verbindungen:

Modul / Dienst	Notwendige Verbindungen
eGK-Lesegerät bei LAN-Anbindung	Die freizugebenden Ports entnehmen Sie bitte dem Informationsmaterial des Herstellers.
DSSIDEX (wird für die Bildübergabe aus dem Röntgenprogramm SidexisXG benötigt)	Am Sidexis-SQL-Server muss der UDP-Port 1434 (eingehend) offen sein. Diese Regel wird normalerweise in der Windows-Firewall unter dem Namen „Sidexis“ durch die Sidexis-Installation erzeugt.
DS-Win-E-Mail-Server (zur Weiterleitung von DS-Win-E-Mail-Konten an andere Anwendungen)	Die Ports können in den Einstellungen selbst festgelegt werden. Standardports sind 25 (SMTP) und 110 (POP3).
DS-Win-Lizenzserver (nur in Praxen mit Einzelmodulen)	- Port 4030 (TCP) auf den Lizenzserver (dslizman.exe)
DS-Win-Talk	- Port 5060 (TCP)
Windows-Dateifreigabe (SMB)	- Ports 137 und 138 (UDP) - Ports 139 und 445 (TCP) - Port 5535 (UDP/TCP)
Windows Remotedesktopdienste	- Port 3389 (TCP/UDP)
Rise KIM-Client-Modul	An dem Rechner wo das Rise KIM-Client-Modul installiert ist, zur Kommunikation von anderen Stationen: - SMTP-Port (selbst konfigurierbar) -> Standard: 465 (TCP) - POP3-Port (selbst konfigurierbar) -> Standard: 995 (TCP)
KIM-Client-Modul anderer Anbieter	Für die Kommunikation von anderen Stationen, sind in der Regel eingehende, selbst konfigurierbare SMTP- und POP3-Ports, an dem Rechner mit installiertem KIM-Client-Modul, freizugeben. Bitte entnehmen Sie die nötigen Firewall-Einstellungen der Dokumentation des Anbieters. Allgemeingültige Hinweise zur Installation finden Sie in unserer KIM-Installationsanleitung auf www.dampsoft.de im Bereich „Service – Infos für Systembetreuer“.

3.3.2. Ausgehende Verbindungen:

Modul / Dienst	Notwendige Verbindungen
DS-Win-Talk	- Port 5060 (TCP)
Rise KIM-Client-Modul	An dem Rechner wo das Rise KIM-Client-Modul installiert ist: - Port 443 (TCP) auf IP des Konnektors [SOAP-Schnittstelle des Konnektors] - Port 389 (TCP) / Port 636 (TCP) auf IP des Konnektors [Verzeichnisdienst (Port 389 ohne TLS / Port 636 mit TLS)] - Port 465 (TCP) auf 100.102.0.0 mit statische Route über die Konnektor IP (die statische Route wird bei der Installation automatisch angelegt) [KIM Fachdienst] - Port 995 (TCP) auf 100.102.0.0 mit statische Route über die Konnektor IP (die statische Route wird bei der Installation automatisch angelegt) [KIM Fachdienst]
KIM-Client-Modul anderer Anbieter	Für die Kommunikation mit dem Konnektor, dem Verzeichnisdienst und dem Fachdienst sind in der Regel ausgehende Verbindungen, an dem Rechner mit installiertem KIM-Client-Modul, notwendig. Bitte entnehmen Sie die nötigen Firewall-Einstellungen der Dokumentation des Anbieters. Allgemeingültige Hinweise zur Installation finden Sie in unserer KIM-Installationsanleitung auf www.dampsoft.de im Bereich „Service – Infos für Systembetreuer“.

DAMPSOFT GmbH
Vogelsang 1
24351 Damp

T 04352 9171-16
F 04352 9171-90
info@dampsoft.de
www.dampsoft.de

Pionier der Zahnarzt-Software.
Seit 1986.

DAMPSOFT
Die Zahnarzt-Software