

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

hmd.[anwenderinfo](#)

Januar 2018

Sehr geehrte hmd-Anwender,

uns erreichen immer mehr Anfragen zur Sicherheit in der Steuerkanzlei. Dabei geht es um die Verbesserung oder Erhöhung des Schutzes durch die auf dem Markt befindlichen Virens Scanner, die die Kanzlei vor Schad-Software und auch Schad-Emails bewahren sollen.

Sicher haben Sie, auf Grund der aktuellen RANSOM Software, auch Ihren IT-Betreuer informiert, um die Sicherheit der Virenschutzsoftware überprüfen, bzw. erhöhen zu lassen. Virens Scanner lassen sich über verschiedene Sicherheitsstufen anpassen. Hierbei treten dann aber Folgeprobleme auf, über die wir Sie informieren möchten.

1. Durch die erhöhten Sicherheitseinstellungen ergeben sich bei der Ausführung der Software Geschwindigkeitseinbußen, die zu Verzögerungen im Laufzeitverhalten führen können.
2. Durch die erhöhten Sicherheitseinstellungen können unter Umständen Programme nicht mehr ausgeführt werden, die einen Start der Software oder die weitere Ausführung verhindern.
3. Durch die erhöhten Sicherheitseinstellungen können Zugriffe auf das Internet blockiert werden, was zur Folge hat, dass Dienste die Daten aus dem Internet beziehen, nicht mehr korrekt funktionieren oder Fehlermeldung auswerfen.
4. Durch die erhöhten Sicherheitseinstellungen können Webseiten nicht mehr korrekt ausgeführt werden.

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Hinweise für den korrekten Einsatz bzw. die Einstellungen für die Ausführung der hmd-Programme am PC oder Server:

Bitte tragen Sie diese Programme in den Ausnahmen der Virens Scanner global ein.

Aufstellung der hmd-Programme, die durch die erhöhten Einstellungen der Virens Scanner mit eingeschalteter **Verhaltensüberwachung** oder **Verhaltenserkennung** aufgefallen sind.

Die Nr. definiert den Ablagepfad, woher die Programme gestartet werden.

Nr.	Programmnamen	Funktion	NEU
5	starter.exe	Winmenü Startprogramm	09/2017
2	cockpit.exe	Personal Cockpit	05/2017
5	hmdprgtm.exe	Zeitmessung Auftragsmanager	05/2017
1	hmdnetvb.exe	Kommunikationsprogramm	05/2017
2	hmd.authserver.exe	Sachbearbeiteranmeldung	05/2017
2	hmd.lilo.exe	Kalender An- und Abmeldung	05/2017
1	hmderg.exe	Erinnerungsmodul	05/2017
1	hmdhtmm.exe	Versenden Email	05/2017
2	hmd.elsterpool.exe	Versand ELSTER	05/2017
1,5	hmdupd2.exe	Updateprogramm	05/2017
2	hmd.fibu.verifizierenbelegmaster.exe	Belegerkennung hmd.skymaster	05/2017
2	hmd.fibu.importbelegmaster.exe	Download Belege hmd.skymaster	09/2017
2	hmd.mailversand.exe	Versenden Emails hmd	05/2017
1	hmdmon.exe	Erstellen Bugreport hmd	05/2017
2	abschluss.exe	hmd.abschluss	05/2017
2	hmd.kanzlei.maileingang.exe	Verwalten Email Eingang	12/2017
5	launcher.exe	Start hmd Umgebung	12/2017

Bitte vergleichen Sie die Liste Ihrer Ausschlüsse von Programmen und Pfaden, falls es zu unkontrollierten Abstürzen der hmd-software kommt.

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Lösungshinweise:

Bitte Sie Ihren IT-Betreuer diese Programme bei Problemen im Virenschanner der Kanzlei bzw. der **Verhaltensüberwachung** oder **Verhaltenserkennung** zu hinterlegen, damit diese Prozesse bzw. Programme **ausgeschlossen** werden.

Programm- oder Verzeichnispfade der hmd-Programme sind wie folgt:

Nr.	Ablagepfad für die Programmausschlüsse im Virenschanner bei Problemen
1	„C:\Program Files (x86)\hmd“ oder „C:\Programme\hmd“
2	„C:\Program Files (x86)\hmd\assemblies“ oder „C:\Programme\hmd\assemblies“
3	<LW>:\winhmd\setup\assemblies
4	<LW>:\winhmd\setup\system32
5	<LW>:\winhmd\programm

Auf den lokalen Arbeitsplätzen und Terminalservern sollten Sie die Pfad-Nr. 1 und 2 komplett aus der Überprüfung vom Virenschanner entfernen. Damit entfallen die Eintragungen der einzelnen Programme.

<LW> betrifft das Netzwerklaufwerk, auf dem die hmd-Installation liegt.

Sollten Sie mehrere hmd-Installation auf Ihrem System haben, betrifft es alle Netzwerklaufwerke, auf denen hmd installiert ist.

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Weitere Lösungshinweise zu Virens Scanner:

Durch die Vielzahl von Virens Scannern ist es uns leider nicht möglich, für jeden Virens Scanner eine korrekte Anweisung zu hinterlegen, wie die Programme oder Ordner ausgeschlossen oder freigestellt werden müssen. Hier hilft Ihnen sicher Ihr IT-Betreuer weiter.

Wichtige Hinweise zu Virens Scanner oder Lösungen:

1. Die Aktualisierung muss automatisch erfolgen. Sowohl von der Software, als auch von den Virensignaturen
2. Die Aktualisierung muss spätestens alle 24 Stunden erfolgen. Besser ist aber alle 3-6 Stunden
3. Die Software sollte eine Verhaltensüberwachung bieten, um Ausbrüche zu erkennen und zu unterbinden
4. Die Software sollte eine Protokollierung über die Ereignisse bieten
5. Die Standardeinstellungen dürfen keine Netzwerklaufrufe scannen und überprüfen
6. Die Standardeinstellungen dürfen keine infizierten Dateien ohne Rückfrage löschen

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Wir haben Ihnen hier eine Liste von Anbietern von Virenlösungen erstellt, die derzeit von uns favorisiert oder nicht favorisiert werden. (Stand 01/2018)

Nr.	Virenlösung	Hinweise zur Lösung bzw. Kundenerfahrungen	Score	Info
1	Panda Adaptive	Wird von hmd zentral verwaltet	+++	04/2017
2	Trend Micro	Gute zentrale Verwaltung und Einstellbarkeit	++	05/2017
3	Avira Pro	Schneller Scanner und einfache Verwaltung	++	05/2017
1	Bitdefender	Zu wenige Erfahrungen	+	10/2017
2	AVG -Antivirus	Sehr starke Ressourcenauslastung	+	10/2017
3	AVAST Pro	Sehr starke Ressourcenauslastung	+	09/2017
4	F-Secure Antivirus	Unübersichtliche Einstellmöglichkeiten	+	06/2017
5	Norman Antivirus	Zu wenige Erfahrungen	+	05/2017
6	Sophos Endpoint Security	Blockiert den PC und Server manchmal zu stark	+	10/2017
7	Microsoft Security	Zu wenige Einstellmöglichkeiten	+	02/2017
8	Avira Personal	Nur für Privatanwender	+	05/2017

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Viren- und Sicherheitslösungen, die in der Vergangenheit negativ aufgefallen sind, bzw. keine Erfahrungswerte vorliegen.

Nr.	Virenlösung	Hinweise zur Lösung bzw. Kundenerfahrungen	Score	Info
1	Kasperski Lab	Löscht ungefragt Dateien	---	12/2017
2	ESET NOD32	Grundeinstellungen zu komplex	--	08/2017
3	McAfee	Zu langsame Engine	--	01/2017
4	GDATA Antivirus	Verbraucht zu viele Systemressourcen	--	01/2017
5	Norton Security Antivirus	Keine globale Verwaltung	---	07/2016
6	eScan Antivirus	Zu viele Fehlalarme	--	03/2017
7	Webroot Antivirus	Keine Informationen	--	11/2017
8	Vipre Antivirus	Keine Informationen	--	11/2017
9	Dr. Web Antivirus	Keine Informationen	--	11/2017
10	Ashampoo Antivirus	Keine Informationen	--	11/2017
11	Outpost Antivirus	Keine Informationen	--	11/2017
12	Zonealarm Antivirus	Keine Informationen	--	11/2017
13	Symantec	Keine Informationen	--	11/2017
14	Ikarus	Keine Informationen	--	11/2017
15	ClamAV / ClamWIN	Keine Informationen	--	11/2017

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Weitere Lösungshinweise für Proxy-Server oder Firewall's mit Virenschanner

Damit auch das Update bzw. die Internetkommunikation zwischen Ihrer hmd.**anwendung** und den hmd.**servern** korrekt funktioniert, müssen in Ihrer Firewall bzw. Ihrem Proxy-Server diese Adresse als Ausnahme hinterlegt werden, falls es zu Problemen kommt.

http://update.hmd-software.com	212.89.151.55	(hmd. update Server)
https://www.hmdweb.net	77.73.249.40	(hmd. portal Server)
https://www.netarchiv.eu	212.89.146.2	(hmd. netarchiv Server)
https://www.hmd-software.com	212.89.151.54	(hmd. mail Server)

Alle ELSTER Server der Finanzverwaltung:

Verfügbarkeit der ELSTER Server: https://www.elster.de/verfuegbarkeit_nw.php

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Ausschlüsse bzw. Freigaben von Ports in der Firewall des Unternehmens:

Standardmäßig müssen folgende **TCP/IP Ports** nach **extern** freigeschaltet werden:

Nr.	Ports	Beschreibung für externe Ports	Ziel-IP
1	80,443	HTTP und HTTPS für den Internetzugang	offen
2	8000	Elsterversand über die Elsterschnittstelle	offen
3	8001	Freigabe bei Nutzung hmd.netarchiv	212.89.146.2
4	8080	Freigabe hmd.skysnc für Kalenderdaten Sync	212.89.146.2
5	9090,9091	Kommunikation mit hmd.skymaster Server	212.89.151.19
6	5440	Kommunikation mit den hmd.webservices	212.89.146.2 77.73.249.40
7	9000-9399	Kommunikation mit dem hmd.portal für die hmd.asp Server Nutzung	77.73.249.40
8	80,443	Kommunikation mit dem hmd.update Server	212.89.151.55
9	25, 110, 143, 465, 587, 993, 995, usw.	Kommunikation per Email mit den externen Mailservern der Kanzlei für der hmd.mail Programme	Zieladresse Mailserver

Weitere Organisations- bzw. Sicherheitsfragen können Sie gerne mit unserer Systemabteilung in Verbindung mit Ihrem IT-Betreuer besprechen.

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Ausschluss der Datenbankverzeichnisse auf Ihrem Server oder PC

Die SQL Datenbanken von hmd sind grundsätzlich im Ordner „database“ auf Ihrem Server oder PC installiert. Diesen Ordner und seine Unterordner können Sie ebenfalls von der Virensuche ausschließen. Dies verbessert die Performance der SQL Datenbanken.

Globales Viren Informationssystem für blockierte Anwendungen

An diesen Stellen im Internet können Sie prüfen und feststellen, ob Programme als „Schadsoftware“ hinterlegt sind.

- 1) <http://www.isthisfilesafe.com/>
- 2) <https://www.virustotal.com/de/>

Nicht jeder Virenschanner erkennt die Software korrekt als „nicht infiziert“ bzw. auch als Schadsoftware.

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Einrichten eines neuen Netzwerkarbeitsplatzes für hmd

Wir empfehlen Ihnen für die Einrichtung eines neuen Arbeitsplatzes / Netzwerkarbeitsplatzes oder Windows Terminal Server folgende Sicherheitseinstellungen:

1. Der Benutzer sollte auf dem PC / Server keine Admin-Rechte mit den normalen Benutzerrechten bekommen.
2. Die UAC (UserAccountControl) sollte auf dem PC / Server immer im Standardmodus, also „aktiv“ sein.
3. Die Windows Firewall ist in Kombination mit dem Virens Scanner korrekt einzustellen. Bringt der Virens Scanner eine Firewall mit, ist die Windows Firewall zu deaktivieren. Ansonsten empfehlen wir die Firewall aktiviert zu lassen. Auf PC oder Servern gelten unterschiedliche Einstellungen.
4. Die DEP (Dateiausführungsverhinderung) von Windows ist zu deaktivieren.
5. Weitere Sicherheitsmaßnahmen können gerne über Gruppenrichtlinien oder andere Mechanismen ausgerollt werden.
6. Windows Update sollten konsequent eingespielt werden. Nutzen Sie dazu den kostenlosen WSUS Server von Microsoft, um die Update im Netzwerk zu verteilen.
7. Zwei Virens Scanner am PC oder Server bieten keine Vorteile, sondern eher Nachteile und Programmabstürze sind vorprogrammiert.
8. Verwenden Sie keine Programme von Anbietern, die Ihnen Aufräumdienste oder Performanceverbesserungen versprechen. Diese Programme zerstören in aller Regel die Registry und damit Ihren PC-Arbeitsplatz.

Sicherheit und Einrichtung eines Arbeitsplatzes in der Steuerkanzlei

Verwendung einer Firewall oder eines Router mit Port Regelungen

Der Sicherheit in Steuerkanzleien und Unternehmen wird fast überall nicht die notwendige Aufmerksamkeit geschenkt. Meist kommt das Thema erst auf den Tisch, wenn ein Schadensfall eingetreten ist, bzw. gehandelt werden muss. Hier einige Empfehlungen von hmd:

Nr.	Firewall Lösung	Hinweise zur Lösung bzw. Kundenerfahrungen	Score	Info
1	Watchguard	Wird von hmd unterstützt und gewartet	+++	04/2016
2	Sophos / Astaro	Kunden setzen diese Firewall ein und haben gute Erfahrungen	++	05/2017
3	Securepoint	Kunden setzen diese Firewall ein und haben gute Erfahrungen	++	05/2017
4	DELL SonicWALL	Kunden setzen diese Firewall ein und haben gute Erfahrungen	++	05/2017
5	Lancom	Kunden setzen diese Firewall ein und haben gute Erfahrungen	++	05/2017
6	ZyXEL	Kunden setzen diese Firewall ein und haben gute Erfahrungen	++	05/2017
1		Alle Typen von Firewalls mit Portfilterung und Paketverwaltung	+	10/2017
1	Fritzbox	Bietet zu wenig Sicherheit	--	10/2017
2	Telekom Speedport	Bietet zu wenig Sicherheit	--	09/2017
3		Alle Firewall und Router ohne Portfilterung und Paketverwaltung	--	06/2017