Newsletter

Sahara AG
Qualität Sicherheit Beratung

Sehr geehrte Kunden der Sahara AG,

das erste Halbjahr hat, bedingt durch Corona und die von Regierungsseite getroffenen Maßnahmen, alle vor besondere Herausforderungen gestellt. Auch wir haben von Mitte März bis Mai unsere Beratungstätigkeit vor Ort komplett eingestellt. Nunmehr sind wohl die schlimmsten Auswirkungen vorbei und langsam beginnt die Umstellung auf die neue Realität.

Wie wir in unserem Weihnachtsnewsletter aus dem Dezember 2019 angekündigt haben, möchten wir Sie regelmäßig über Themen zum Datenschutz informieren. Leider ist der erste Newsletter für das 1. Quartal ausgefallen, aber wir versuchen die Informationen in den weiteren Newslettern nachzuholen.

In diesem Newsletter möchten wir Sie etwas ausführlicher zum Thema Datenschutz unter Windows 10 informieren.

Viel Spaß bei der Lektüre wünscht Ihnen

Ihre Sahara AG

Datenschutz unter Windows 10

1 Allgemeines

Neben mehreren anderen Einstellungsmöglichkeiten unter Windows 10 wollen wir uns hier speziell mit den Themen Firewall, Virenscanner und Verschlüsselung beschäftigen.

Alle Rechner mit dem Betriebssystem Windows 10 sind mit einer Firewall (Windows Firewall), einem Virenscanner (Bitdefender) und einer Verschlüsselung (Bitlocker) ausgestattet. Zusätzlich können Datenschutzeinstellungen für Original ï Windowsprogramme vorgenommen werden. Die Aktualisierung erfolgt über die ständigen Updates von Microsoft. Diese Sicherheitseinrichtungen sind von den Datenschutzbehörden als zulässige und ausreichende Maßnahmen eingestuft worden. Lediglich ein gesetzlicher Zugang (Hintertürchen) durch US-Behörden (z. B. NSA) ist vorhanden, allerdings für die normalen Nutzer nicht relevant.

Wichtig: Grundsätzlich können die Einstellungen auf allen Windows 10 Rechnern vorgenommen werden, außer auf einem Server mit einem Warenwirtschaftssystem oder auf Rechnern, die auf das Warenwirtschaftssystem zugreifen.

Je nach Warenwirtschaftssystemanbieter werden die Standards von Windows 10 genutzt, gezielt ausgeschlossen oder durch andere Soft- und Hardware ersetzt. Wenn auf diesen Rechnern Änderungen vorgenommen werden sollen, muss dies unbedingt vorher mit dem jeweiligen Warenwirtschaftssystemanbieter abgesprochen oder geklärt werden, welche Einstellungen gemacht werden können. Teilweise ist der übliche Benutzer für das Warenwirtschaftssystem so weit eingeschränkt, dass diese Einstellungsmöglichkeiten gar nicht zur Verfügung stehen. In der Regel hat jedoch der Administrator alle Rechte für alle Einstellungen.

Registergericht: Amtsgericht Gießen HRB 3510
Vorstand: Doris G. Hohenwald, Jochen D. Hohenwald
Aufsichtsrat: Thomas Richter (Vorsitzender)

Commerzbank AG Filiale Gießen
IBAN: DE14 5134 0013 0203 0609 00
BIC: COBADEFFXXX

Sahara Qualität Sicherheit Beratung Aktiengesellschaft ï Finkenweg 1 ï 35415 Pohlheim
www.sahara-ag.de ï info@sahara-ag.de ï Telefon +49 6404 66 86 935 ï Telefax +49 6404 66 86 934

2 Sicherheitseinstellungen

Ihr Weg dorthin:
- Links unten auf das Microsoftsymbol klicken (linke Maustaste).
- Auf das Zahnrad (Einstellungen) klicken (linke Maustaste).
- Auf dem Einstellungsmenu nach unten rollen und auf Datenschutz (linke Maustaste) klicken).

Über den Datenschutz lassen sich Zugriffe auf Daten und Geräte entsprechend Ihren Wünschen einstellen. Jedoch werden diese Einstellungen nur von Microsoft-Programmen berücksichtigt, andere Programme können diese Einstellungen ignorieren. Sie können die einzelnen Punkte nacheinander abarbeiten und die Einstellungen anpassen.

Beispiel:
Sie können den Zugriff auf Ihre Kamera nur durch das Abkleben absolut sicherstellen, obwohl Sie den Zugriff ausgeschlossen haben.

Beispiel:
Sie blockieren Ihre Standortabfrage und somit auch Programme die Ihren Standort benötigen (Wetter usw.)

In der Regel werden aber die Programme dieses Problem anzeigen oder sogar nach der Freigabe (Ausnahme von der Regel) fragen. Sie können natürlich jederzeit die Einstellungen wieder zurücksetzen.

3 Firewall

Ihr Weg dorthin:
- Links unten auf das Microsoftsymbol klicken (linke Maustaste).
- Auf das Zahnrad (Einstellungen) klicken (linke Maustaste).
- Auf dem Einstellungsmenu auf Netzwerk und Internet (linke Maustaste) klicken,
- Prüfen, ob im rechten Feld als Überschrift ĂStatusñerscheint,
- Wenn ja, herunterrollen und auf ĂWindows Firewallñ(linke Maustaste) klicken).

Die Firewall blockiert unerwünschte Daten aus externen Netzwerken. In der Übersicht werden die vorhandenen Netzwerke mit ihrem Status (Firewall aktiviert und aktuell genutztes Netzwerk (aktiv)) angezeigt. Mit einem Klick mit der linken Maustaste können Sie die jeweilige Firewall aktivieren oder deaktivieren. Durch das Aktivieren verwenden Sie Standardeinstellungen von Microsoft, welche bereits bestimmte Apps und Programme von der Blockade durch die Firewall ausgenommen haben.
Falls von Ihnen gewünschte Programme durch die Firewall blockiert sind, können über dieses Menu Apps oder Programme zugelassen werden.

4 Verschlüsselung

Ihr Weg dorthin:

- Öffnen Sie den Explorer und klicken Sie mit rechten Maustaste auf das Laufwerk C:
- Auf dem kleinen Menu klicken Sie auf Bitlocker einrichten oder Bitlocker verwalten
- Es werden Ihre eigenen verfügbaren Laufwerke angezeigt.
- Im unteren Bereich steht die Option ÄWechseldatenträger ï BitLocker To Goñzur Verfügung, mit der Sie Ihre externen Datenträger, die über USB mit Ihrem Rechner verbunden sind, verschlüsseln können.

Die Verschlüsselung von lokalen Datenträgern schützt die lokalen Festplatten und Partitionen vor unberechtigtem Zugriff und vor dem Auslesen der Daten (z. B. nach Ausbau der Festplatte). Die Verschlüsselung ist nur bis zur erfolgten Anmeldung am System (mit oder ohne Passwort) aktiv, d. h. es handelt sich hier um eine reine Hardwareverschlüsselung.

Achtung: Den Verschlüsselungsvorgang auf keinen Fall unterbrechen (Stromausfall ï Akku oder Netz), da sonst die auf dem Datenträger (Festplatte, Partition oder USB-Stick) bereits vorhandenen Daten verloren gehen können. Die Daten sind zwar noch vorhanden, können aber nicht entschlüsselt werden.
Tipp: Externe Datenträger immer zuerst verschlüsseln, bevor Daten dort gespeichert werden oder vor dem Verschlüsseln immer zuerst eine Datensicherung durchführen!

Verschlüsseln von Wechseldatenträgern:

Generell können Wechseldatenträger wie USB-Sticks oder (externe) Festplatten, mit ÄBitlocker to Goñverschlüsselt werden. Der verschlüsselte Datenträger kann anschließend von jedem System mit Windows 7-10 gelesen werden.

- Gehen Sie gemäß Ähr Weg dorthinñvor, um Bitlocker to go aufzurufen.
- Nach dem Aktiveren von BitLocker To Go durch Klick auf das Wechselträgerlaufwerk, erhalten Sie die Auswahl der Methode zum Entsperren des Laufwerks nachdem das Laufwerk verschlüsselt wurde.
- Wählen Sie die Option Kennwort und denken Sie sich ein **sicheres** Kennwort aus.
- Danach führt Sie das System zur Erstellung des Wiederherstellungsschlüssels. Diesen sollten Sie auf Ihrem persönlichen Laufwerk abspeichern und ggfs. zusätzlich ausdrucken.
- Wählen Sie nachfolgend die passenden Optionen aus.
- Der Verschlüsselungsmodus ist bereits auf Kompatibilität voreinstellt (diesen bitte nicht verändern).
- Starten der Verschlüsselung.

Sobald Sie beim nächsten Mal den USB-Stick an Ihrem System anschließen, werden Sie nach dem Passwort gefragt, um den USB-Stick zu entsperren. Haben Sie das Passwort vergessen, so können Sie über ÄWeitere Optionenñdurch Eingabe des Wiederherstellungsschlüssels den Datenträger entsperren. Dieser ist praktisch ein zweites Passwort, falls das erste vergessen wurde. Sie können mehrere USB-Stick mit dem gleichen Passwort versehen (z. B. für die Datensicherung), jedoch hat jeder USB-Stick einen anderen Wiederherstellungsschlüssel.

Ebenso können Sie über ĂWeitere Optionenñdie automatische Entschlüsselung einrichten. Dies bedeutet, dass dieser USB-Stick nur auf dem Rechner automatisch entschlüsselt wird. Auf anderen Rechnern muss er mit dem Passwort entschlüsselt werden. Jedoch können auf anderen Windows 10 Rechnern nach oder bei Eingabe des Passwortes die automatische Entschlüsselung eingerichtet werden.

Falls Sie verschlüsselte USB-Sticks für die Datensicherung verwenden möchten, sollten diese auf dem entsprechenden Rechner automatisch entsperrt werden, da sonst die Datensicherung nach einem eventuellen Neustart nicht funktionieren würde.

5 Virenscanner (Bitdefender)

Ihr Weg dorthin:
- Links unten auf das Microsoftsymbol klicken (linke Maustaste).
- Auf das Zahnrad (Einstellungen) klicken (linke Maustaste).
- Auf dem Einstellungsmenu auf Update und Sicherheit (linke Maustaste) klicken und auf Windows Sicherheit (linke Maustaste) klicken).

Dort können Sie direkt eine Überprüfung vornehmen und generelle Einstellungen vornehmen.

Wichtige Einstellungen unter Viren- & Bedrohungsschutz.
- Sie können jederzeit eine Überprüfung durchführen (Schnellüberprüfung). Diese dauert nur wenige Minuten. Zusätzlich können Sie im Unterpunkt Scanoptionen drei weitere Prüfmöglichkeiten auswählen. Diese können deutlich länger dauern und zu einem Neustart des Rechners führen.
- Einstellungen für Viren- & Bedrohungsschutz ï Einstellungen verwalten (**Empfehlungen**):
  - Echtzeitschutz ï ein
  - Cloudbasierter Schutz ï ein
  - Automatische Übermittlung von Beispielen ï ein
  - Manipulationsschutz ï ein
  - Benachrichtigungen (Benachrichtigungseinstellungen ändern) ï alle ein

6 Hinweis (Wiederholung von Seite 1)

Wichtig: Grundsätzlich können die Einstellungen auf allen Windows 10 Rechnern vorgenommen werden, außer auf einem Server mit einem Warenwirtschaftssystem oder auf Rechnern, die auf das Warenwirtschaftssystem zugreifen.

Je nach Warenwirtschaftssystemanbieter werden die Standards von Windows 10 genutzt, gezielt ausgeschlossen oder durch andere Soft- und Hardware ersetzt. Wenn auf diesen Rechnern Änderungen vorgenommen werden sollen, muss dies unbedingt vorher mit dem jeweiligen Warenwirtschaftssystemanbieter abgesprochen oder geklärt werden, welche Einstellungen gemacht werden können. Teilweise ist der übliche Benutzer für das Warenwirtschaftssystem so weit eingeschränkt, dass diese Einstellungsmöglichkeiten gar nicht zur Verfügung stehen. In der Regel hat jedoch der Administrator alle Rechte für alle Einstellungen.