Nutzung der HIZ-IT im Homeoffice

Dieses Dokument erklärt in Kurzform, welche Voraussetzungen ein Homeoffice-Arbeitsplatz erfüllen muss, um die vom HIZ an der Universität des Saarlandes zur Verfügung gestellte IT-Infrastruktur zu nutzen und erklärt die ersten Schritte dazu.
Bitte beachten Sie, dass diese Ausführungen weder für Beschäftigte an der HTWsaar, noch an den Universitätskliniken Gültigkeit haben!

Voraussetzungen

Ihr Arbeitsplatz im Homeoffice muss – aus Sicht der IT – folgende Voraussetzungen erfüllen:

- Vorhandensein eines dienstlichen, mobilen Endgerätes mit dem Betriebssystem Windows 10
- Ein installierter und aktivierter Virenwächter, das HIZ empfiehlt Microsoft Defender
- Ein privater Internet-Zugang (DSL, LTE o.ä.) mit unbegrenztem Datenvolumen (Flatrate)
- Ein installierter VPN-Client Cisco AnyConnect (s.u.)
- Benötigte Anwendungssoftware nach Bedarf, z.B.
    - Microsoft Office
    - SAP-Client
    - Client für das D3-Dokumenten-Management-System
- Verständnis für besonders vorsichtiges Verhalten bzgl. Virengefahren.

Vorbereitung

1. Beantragen einer persönlichen IP-Adresse für den VPN-Zugang

Sofern noch nicht erfolgt, müssen Sie eine persönliche IP-Adresse für den VPN-Zugang beantragen. Diese dient dazu, eine verschlüsselte Verbindung zur Universität aufzubauen und die benötigten Ressourcen zugreifbar zu machen.

Für Beschäftigte in der UdS-Verwaltung: Für Sie wurden bereits Kennungen von Ihren Dezernatsleitern beantragt. Sie brauchen nichts zu tun.

Für sonstige Beschäftigte: Nutzen Sie das Formular unter der Adresse
https://www.hiz-saarland.de/dienste/persoenliche-ip-adresse-fuer-den-vpn-zugang-der-uds/
Füllen Sie es bitte komplett aus.

2. Installation des VPN-Clients Cisco AnyConnect

(Auf Notebooks der Verwaltung ist dieses Programm bereits installiert.)

Sofern der VPN-Client noch nicht auf Ihrem Gerät installiert ist, müssen Sie dies tun – Sie benötigen dazu das Administratoren-Passwort Ihres PCs. Die Installation geht wie folgt:
- Laden Sie zunächst das Installationsprogramm von folgender Seite:
  https://www.hiz-saarland.de/dienste/vpn/
  Sie müssen sich hierzu mit Ihrer HIZ-Kennung/UdS-Kennung nebst Passwort anmelden.
- Starten Sie das Installationsprogramm anyconnect-win-latest.msi, das sich nun in Ihrem Downloadordner befinden sollte.
- Bestätigen Sie alle Abfragen des Programmes mit „Accept“ bzw. „next“ oder „ok“.
- Bestätigen Sie auch die Abfrage nach Änderungen an Ihrem Gerät mit „ja“.
- Geben Sie auf Anfrage auch Ihr Administratorenpasswort ein.
- Nach dem „Finish“-Knopf ist das Programm installiert.

Start einer Telearbeit-Sitzung

***(Für Beschäftigte in der UdS-Verwaltung:** Auf Ihrem Desktop ist eine PDF-Datei namens „Anleitung“ abgelegt, die eine Verbindungs-Anleitung beinhaltet.)*

1) Verbinden Sie Ihren gestarteten PC mit Ihrem häuslichen Internet-Zugang.

2) Starten Sie den VPN-Client:
- Geben Sie im Windows-Suchfeld „anyconnect“ ein.
- Starten Sie aus den Suchergebnissen das Programm „Cisco AnyConnect Secure Mobility Client“.
- Geben Sie nach der Meldung „Ready to connect“ den Namen eines unserer VPN-Server ein:
  asa1.uni-saarland.de oder asa2.uni-saarland.de
  und klicken Sie auf „connect“
- Melden Sie sich mit Ihrer HIZ-Kennung/UdS-Kennung („username“) nebst Passwort an – klicken Sie auf „OK“

Sie sind nun über eine verschlüsselte Verbindung mit dem Netzwerk der Universität verbunden. Bei den kleinen Symbolen unten rechts am Bildschirm ist ein neues Symbol zu finden, ein Ball mit einem Vorhängeschloss.

Sicherheitshinweis: Bitte beachten Sie, dass Sie nun eine Verbindung zwischen dem einigermaßen sicheren Netzwerk der Universität und dem eher als unsicher anzusehenden Netzwerk Ihres Internet-Providers darstellen. Gehen Sie daher bitte besonders sorgsam vor. Einige Ratschläge:
- Benutzen Sie keine Office-Dateien, die kein „x“ in der Namenserweiterung haben. Word-Dateien im .doc-Format sind grundsätzlich virengefährdet, verwenden Sie stattdessen das modernere Format .docx – das gleiche gilt für Excel- und Powerpoint-Dateien.
- Öffnen Sie **keinesfalls** Dateien dieser gefährdeten Typen, die Sie per E-Mail erhalten, auch nicht, wenn sie vermeintlich von Ihren Vorgesetzten oder guten Kollegen oder Freunden kommen. Bitten Sie solche Personen, Ihnen die Dateien noch einmal im modernen Format zu senden.

3) Verbinden Sie bei Bedarf die von Ihnen benötigten Server-Laufwerke

Für Beschäftigte in der UdS-Verwaltung: Für Sie sind Verknüpfungen zu den benötigten Laufwerken auf dem Desktop abgelegt: dvont01, itm2k01, home.
Sie können diese jeweils durch Doppelklick aktivieren.
(Falls nach Benutzername und Passwort gefragt wird, müssen Sie hier Ihre univw-Kennung in der Form univw\<nachname> und das dazugehörige Passwort eingeben.)

Für sonstige Beschäftigte: Sinnvollerweise notieren Sie vor Antreten der Arbeit im Homeoffice die auf Ihrem „normalen“ Arbeits-PC genutzten Netzwerklaufwerke und verbinden diese über die Funktionen des Betriebssystems.

4) Starten Sie Ihre benötigten Anwendungsprogramme

Abschluss einer Telearbeit-Sitzung

1) Schließen Sie Ihre Anwendungsprogramme.

2) Trennen Sie die verbundenen Server-Laufwerke (optional).

3) Schließen Sie die VPN-Verbindung:

- Rechts-klicken Sie auf das VPN-Symbol rechts unten am Bildschirm (ein Ball mit einem Vorhängeschloss)
- Klicken Sie auf „Disconnect“.