Empfehlungen zum Arbeiten im Homeoffice

Das Arbeiten im Homeoffice bringt Risiken und Herausforderungen verschiedener Art mit sich. Folgende Empfehlungen erstrecken sich auf die Bereiche IT-Nutzung, allgemeine Informationssicherheit und Nutzung von externen Diensten.

Technische Empfehlungen/ IT-Nutzung

- Nutzen Sie sichere Passwörter. Richtlinien hierfür finden Sie auf unseren Webseiten unter www.rz.uni-kiel.de/go/pwrl
- Achten Sie im Homeoffice auf eine passwortgesicherte, verschlüsselte Konfiguration Ihres WLAN (bspw. WPA2-Verschlüsselung).
- Verwenden Sie niemals dienstlich genutzte Passwörter für externe Angebote.
- Sorgen Sie dafür, dass Ihr Rechner mit einer aktuellen Virenschutz-Software ausgestattet ist. Für Dienst-Rechner verwenden Sie die Software Sophos Antivirus, die Sie auch auf Ihrem privaten Endgerät verwenden dürfen www.rz.uni-kiel.de/go/antivirus.
- Achten Sie auf eine aktivierte Firewall.
- Achten Sie darauf, dass Ihr System und die verwendete Software aktuell sind. Führen Sie regelmäßig Updates durch.
- Verwenden Sie für Datenaustausch und Datensicherung die Fileservices und Dienste des Rechenzentrums. Sollten Sie dennoch Ihre Daten auf lokale, externe Medien kopieren müssen, schließen Sie diese nur zum Zweck der Kopie-Erstellung an. Mobile Endgeräte und Datenträger sind immer zu verschlüsseln.
- Vorsicht vor Phishing-Mails! Seien Sie stets aufmerksam beim Umgang mit empfangenen E-Mails:
    - Öffnen Sie keine Anhänge aus E-Mails von unbekannten Absendern oder von Absendern, von denen Sie keine entsprechende E-Mail erwarten.
    - Klicken Sie niemals auf Links, ohne zuvor die Vertrauenswürdigkeit der eingegangenen Mail sowie über den Tooltip die tatsächliche Ziel-Adresse des Links zu prüfen.
    - Löschen Sie grundsätzlich E-Mails, die Ihr Misstrauen erregen.
    - E-Mails, in denen zur Eingabe von persönlichen Daten, Passwörtern o.ä. auf einer verlinkten Webseite aufgefordert wird, sind höchst bedenklich und sehr wahrscheinlich Phishing-Attacken.
    - Diese Vorsicht gilt nicht nur bei E-Mails, sondern auch SMS, Social-Media-Inhalten, per Messenger verbreiteten Nachrichten etc.
- Bei der Klärung von Auffälligkeiten kann auch der RZ-Helpdesk kontaktiert werden: www.rz.uni-kiel.de/de/hotline.

Weiterführende und aktualisierte Informationen finden Sie auf den Seiten des Rechenzentrums unter www.rz.uni-kiel.de/faq und www.rz.uni-kiel.de/de/faq-homeoffice.

Allgemeine Informationssicherheit

Auch allgemeine Vorsichtsmaßnahmen sind nötig, um den Schutz von personenbezogenen Daten und

vertraulichen dienstlichen Informationen gewährleisten zu können. Folgende Empfehlungen gelten insbesondere, wenn zum Homeoffice mehr als eine Person Zutritt hat. Unbefugte Einsichtnahme dienstlicher Informationen durch Dritte (z.B. Familienmitglieder, Partner*in, Besucher*in, etc.) ist zu verhindern.

- Nutzen Sie wenn möglich ein separates Arbeitszimmer, dessen Sicherheitsniveau (abschließbarer Schreibtisch/Schrank) mit dem des dienstlichen Büroraums vergleichbar ist.
- Lassen Sie Datenträger und dienstliche Unterlagen nicht unbeaufsichtigt und schließen Sie diese nach Dienstende weg.
- Für den Fall, dass dienstliche Datenträger bzw. Unterlagen transportiert werden müssen, z. B. vom Büro ins Homeoffice, führen Sie diese nur in verschlossenen Behältnissen mit. Der Verlust dienstlicher Datenträger bzw. Unterlagen ist dem/der Vorgesetzten unverzüglich anzuzeigen.
- Sperren Sie Ihren Laptop, wenn Sie nicht daran arbeiten und verschlüsseln Sie diesen.
- Bei Verlust von mobilen Endgeräten ist eine unverzügliche Verlustmeldung an das Rechenzentrum nötig, damit schnell Maßnahmen wie das Sperren von Zugängen und Ändern von Passwörtern ergriffen werden können.
- Führen Sie dienstliche Telefonate mit Personenbezug so, dass Dritte nicht mithören können.
- Vertrauliche Informationen müssen sicher entsorgt werden! Werfen Sie diese nicht in den Hausmüll, sondern bewahren Sie sie abgeschlossen auf und entsorgen sie bei Gelegenheit fachgerecht in der Universität.

Nutzung von externen Diensten

Angesichts des immensen Angebots von externen Diensten und der gewohnten privaten Nutzung mag es naheliegen, diese auch für dienstliche Zwecke im Homeoffice zu verwenden. Bei externen Anbietern offenbaren sich jedoch folgende potenzielle Risiken, weswegen dringend zu empfehlen ist, für dienstliche Zwecke die vom CAU-Rechenzentrum angebotenen Standard-Dienste (bspw. auch CAU-Cloud, www.rz.uni-kiel.de/de/angebote/storage/cau-cloud) zu nutzen:

- Grundsätzlich ist die Nutzung externer Dienste für dienstliche Zwecke nur dann zulässig, wenn die CAU einen Vertrag zur Auftragsverarbeitung mit dem Diensteanbieter geschlossen hat.
- Es ist darauf zu achten, ob der externe Cloud-Dienst eine Transportverschlüsselung anbietet. Diese liegt vor, wenn im Webbrowser der jeweiligen Webadresse ein „https" statt „http" vorangestellt ist und ein SSL- bzw. TLS-Zertifikat vorliegt (dies wird z.B. bei Firefox durch das grüne Schlosssymbol angezeigt). Wird eine Datei hochgeladen und die Übertragung erfolgt nicht verschlüsselt, kann sie theoretisch von Unbefugten eingesehen werden. Ein weitergehender Schutzmechanismus ist die Ende-zu-Ende-Verschlüsselung, deren Einsatz bei sensiblen Inhalten zu empfehlen ist. Im Gegensatz zur Transportverschlüsselung wird hier nicht der Kanal geschützt („Tunnel"), sondern der Inhalt selbst. So kann bspw. beim E-Mailversand die E-Mail ausschließlich vom Sender und Empfänger im Klartext gelesen werden, wenn diese über den entsprechenden Schlüssel verfügen.
- Generell sollte man Informationen zur Authentisierung wie Benutzername und Passwort nicht gespeichert im Browser hinterlegen, sodass sie automatisch beim Aufrufen des Cloud-Dienstes verwendet werden.

Das Löschen von Daten bei Beendigung des Dienstes erfolgt nicht direkt und endgültig; oft werden Kopien der Daten in verschiedenen Rechenzentren gespeichert und nach der Kündigung des Cloud-Dienstes noch eine gewisse Zeit behalten.
Der Standort des Sitzes sowie der Rechenzentren des externen Cloud-Anbieters ist meist unklar bzw. nicht direkt ersichtlich, oft befinden sich die Server im Ausland. Besonders kritisch zu sehen sind Drittstaaten außerhalb der EU ohne angemessenes Datenschutzniveau im Sinne der DSGVO, da die Zugriffsrechte und Datenschutzbestimmungen dort weiter sein können und dem Cloud-Anbieter entsprechend große Nutzungsrechte an den Daten eingeräumt werden. Insbesondere im Hinblick auf dienstliche Daten und dienstliche Regelungen kann das zu unerwünschten Auswirkungen führen.

Für die Dienste des CAU-Rechenzentrums ist gesichert, dass diese insbesondere auch bei Rückgriff auf kommerzielle und nicht-kommerzielle Lösungen von Drittanbietern im Sinne der Landesdatenschutzkonzepte rechtskonform genutzt werden können.

Gehe zu...

- Allgemeine Informationssicherheit
- Nutzung von externen Diensten