

Informationssicherheit und Datenschutz

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)
FORSCHUNGSGRUPPE SECURITY · USABILITY · SOCIETY (SECUSO)

KIT Vorgaben und Informationen

■ Vorgaben

- IuK-Ordnung des KIT
https://www.kit.edu/downloads/AmtlicheBekanntmachungen/2013_AB_036.pdf
- IT-Sicherheitskonzept des KIT <https://s.kit.edu/it-sicherheitskonzept>
- Richtlinie „Aufgeräumter Arbeitsplatz“ des KIT
https://www.isb.kit.edu/downloads/Regelungen/20210222_Richtlinie_Aufgeraumter-Arbeit.pdf
- Absolvieren der Datenschutzschulung (de/en) und Umsetzung der Inhalte
- ...

■ Informationen

- Flyer „Praxistipps IT-Sicherheit“ (relevante Themen/Vorgaben) <https://s.kit.edu/it-sicherheit.praxistipps.flyer;>
- Pro Themengebiet dort Links zu weiterführenden Informationen
-



Hinweise zu dieser Präsentation

- Auswahl der aus unserer Sicht wichtigsten Themen, entsprechend kein Anspruch auf Vollständigkeit
- Verantwortung wird thematisiert, wenn sie für verschiedene Gruppen unterschiedlich ist
- Wer kein mobiles Gerät hat, über das auf die KIT Infrastruktur zugegriffen wird, für den gelten nicht alle der Punkte
- „Geräte“ im Folgenden bezieht sich auf Geräte, über die auf die KIT Infrastruktur zugegriffen wird, z.B. E-Mails abgerufen werden
- Nicht spezifisch für ITBs
- Voraussetzung: Bekannt wer ITBs sind 😊

Sichere Passwörter zur Absicherung von KIT Benutzerkonten und Geräten



Wer Ihr Passwort kennt oder erraten kann, hat Zugang zu den gleichen Daten/ Informationen/ Diensten/Geräten wie Sie & kann z.B. in Ihrem Namen E-Mails versenden.

- Wahl eines sicheren Passworts für *das* KIT Benutzerkonto (ggf. auch weitere KIT spezifische Dienste)
 - Möglichst lang: Mindestens 8 Zeichen, besser 12
 - Kein Passwort (auch nicht leicht abgewandelt), das Sie außerhalb des KIT nutzen
 - Für verschiedene Benutzerkonten unterschiedliche Passworte
 - Passwort-Manager

- Umgang mit Ihren sicheren Passwörtern
 - Nicht rausgeben, auch nicht gegenüber Vorgesetzten, Sekretariaten, ITBs, SCC Mitarbeitern, Kollegen, Freunden, Angehörigen oder Partnern
 - Nicht beobachten lassen bei der Eingabe

Risiko für Identitätsdiebstahl und Befall von Schadsoftware reduzieren (1)

- Antivirussoftware auf allen Geräten
 - Windows (u.a. Sekretariate): Auslieferung mit aktiviertem Windows Defender
 - macOS: Verweis auf SCC <https://www.scc.kit.edu/dienste/6949.php>; jeder selbst verantwortlich
 - Linux: Jeder selbst verantwortlich
 - IOS: Jeder selbst verantwortlich / keine Lösung verfügbar
 - Android: Jeder selbst verantwortlich
- Updates der Betriebssystem- und Anwendungssoftware / Apps
 - PC/Laptop der Sekretariate: ITBs kümmern sich
 - Sonstige Geräte: Jeder selbst verantwortlich
- Betrügerische Nachrichten erkennen
 - Freiwillige Ilias Schulung <https://s.kit.edu/it-sicherheit.betrueg-nachrichten.schulung>
 - Videos, Flyer, Poster für die Büros https://secuso.aifb.kit.edu/betruegerische_nachrichten_erkennen.php



1. Regel: Prüfen Sie Absender und Inhalt jeder Nachricht auf Plausibilität.
✗ Absender: shop@yap.de bei einer SECUSO E-Mail
✓ Absender: net@shop@secuso.de bei einer SECUSO E-Mail

2. Regel: Machen Sie sich damit vertraut, wo Sie die tatsächliche Webadresse hinter einem Link (z. B. am PC oder Laptop im Tooltip oder in der Statusleiste) finden.

3. Regel: Identifizieren Sie den Web-Bereich in der Webadresse (fett und farbig markiert) <https://shop@secuso.org/login>

4. Regel: Prüfen Sie, ob der Web-Bereich zur (vermeintlich) legitimen Nachricht passt.
✓ <https://www.mein-paketenservice.de/>
✗ <https://www.mein-paketenservice.de/shopping-im-web.de/>
✗ <https://shoppen-im-web.de/online-paketenservice.de/>
✗ <https://www.2013.1322-secure.org/secure-logout/>



5. Regel: Prüfen Sie, ob der Web-Bereich korrekt geschrieben ist.
✓ <https://www.baummarkt-total.de/>
✗ <https://www.baummarkt-total.de/>
✗ <https://www.baummarkt-total.de/>
✗ <https://www.baummarkt-total.de/>

6. Regel: Wenn Sie den Web-Bereich nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mittels einer Suchmaschine.
✓ <https://www.secuso.org/>
✗ <https://www.secuso-research.org/>

7. Regel: Prüfen Sie das Dateiformat des Anhangs.
✗ Ausführbare Formate z. B. exe, bat, cmd
✗ Dateien mit Makros z. B. Office Dateien wie doc, docx, docm

8. Regel: Wenn Sie den Anhang nicht eindeutig beurteilen können oder unsicher sind, ob Sie genau dieses Format vom Empfänger erwarten, sollten Sie weitere Informationen einholen, z. B. mittels Kontaktaufnahme. Nutzen Sie dafür sich die Kontaktdaten aus der E-Mail oder dem Anhang.

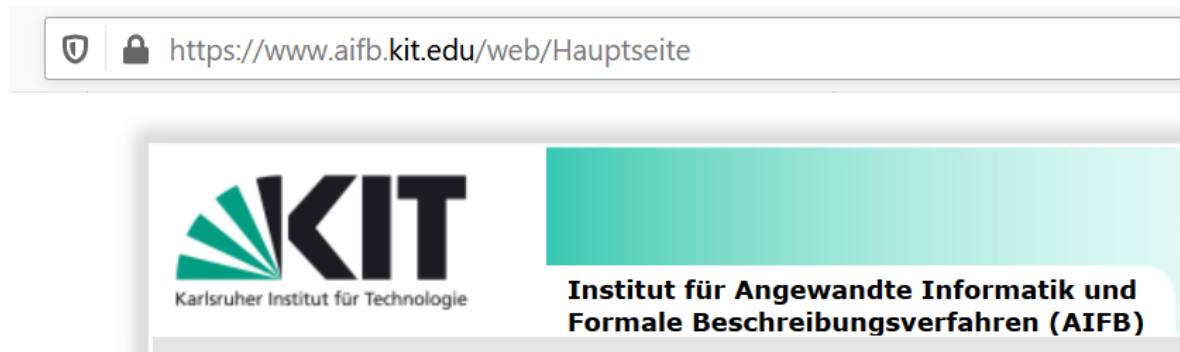
© 2022 Die Inhalte sind urheberrechtlich geschützt. Die Verwendung der Inhalte erfolgt im Rahmen der AIFB-Initiativen. Die Weiterverbreitung ist ohne schriftliche Genehmigung der AIFB untersagt.




KIT - die Fachuniversität der Welt www.kit.edu

Risiko für Identitätsdiebstahl und Befall von Schadsoftware reduzieren (2)

- Keine *fremden* Datenträger/ Kabel an Geräte anschließen
- VPN außerhalb des KIT Netz (Netzwerkkabel am KIT oder KIT WLAN)
 - PC/Laptop der Sekretariate: ITBs kümmern sich um Installation und Einrichtung
 - Windows: Auslieferung mit installiertem Open VPN Client, jeder ist (noch) selbst für die Einrichtung verantwortlich
 - macOS/Linux/ IOS/ Android: Verweis auf SCC <https://www.scc.kit.edu/dienste/openvpn.php> jeder ist selbst verantwortlich
- HTTPS verwenden (wann immer möglich) und Domain (fett hinterlegt) prüfen



Risiko für Datenschutzvorfälle und Verletzung von anderen Geheimhaltungsvorgaben reduzieren (1)

- Verschlüsselung von Daten auf Endgeräten
 - PC/Laptop der Sekretariate: ITBs kümmern sich
 - Windows: Auslieferung mit Bitlocker *zukünftig* durch ITBs
 - macOS/Linux: Jeder selbst verantwortlich
 - iOS: Jeder selbst verantwortlich / bei Lieferung von Apple bereits aktiviert
 - Android: Jeder selbst verantwortlich
- Verschlüsselung von schützenswerten Daten/Informationen auf mobilen Datenträgern (z.B. USB) <https://www.scc.kit.edu/dienste/7910.php>
- E-Mails verschlüsseln (Datenschutzanforderung (!)) und signieren auf Basis von S/MIME-Nutzerzertifikat der KIT-Certification Authority
 - PC/Laptop der Sekretariate: ITBs kümmern sich
 - Sonstige Geräte: Jeder selbst verantwortlich
- Prüfen, ob die entsprechenden Daten bei dem jeweiligen *Cloud-/Online-Dienst* abgelegt werden dürfen
 - Entscheidungshilfe für die bekanntesten Dienste www.scc.kit.edu/dienste/clouddienste.php
 -  bw Sync & Share

Risiko für Datenschutzvorfälle und Verletzung von anderen Geheimhaltungsvorgaben reduzieren (2)

- Sicherer Umgang mit schützenswerten Daten / Informationen
 - Solche Informationen nur bewusst und sparsam an Externe geben
 - Verteilerkreise klein halten
 - Unterlagen nur so lange wie nötig aufbewahren
 - Nicht mehr benötigte Datenträger inkl. Papier sachgerecht vernichten
 - Nicht mehr benötigte Daten auf mobilen Geräten löschen
 - Mit der Rückgabe von Geräten die Daten darauf sicher löschen
 - Wenn HiWis keine KIT Laptops haben, dort keine personenbezogenen Daten verarbeiten lassen
 - Keine E-Mail Weiterleitung einrichten

- Dienstliche Mails nur über KIT-Account verschicken
- Mails an Studierende nur an deren KIT-Adresse schicken
 - bei Mails von externen Adressen um nochmalige Zusendung von interner Adresse bitten

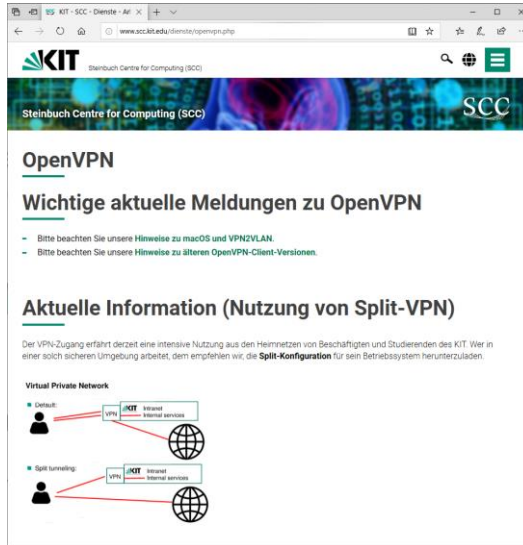
Auch dies gilt insbesondere für studentische und wissenschaftliche Hilfskräfte

Risiko für IT-Sicherheits- und Datenschutzvorfälle im Büro reduzieren

- Einsicht in personenbezogene, vertrauliche, persönliche Informationen auf Befugte begrenzen
- Bildschirm und Unterlagen vor unberechtigten Blicken schützen (auch mobil)
- Beim Verlassen des Arbeitsplatzes Bildschirm sperren oder abmelden, inkl. automatische Bildschirmsperre nach 5 Minuten an normalen IT-Arbeitsplätzen bzw. nach 1 Minute bei Smartphones, Tablets u. ä.
- Bildschirmbenachrichtigungen mit möglicherweise schützenswerten Informationen in Sperrbildschirmen ausschalten
- Räume und ggf. Fenster beim Verlassen abschließen
- Öffentliche Räume aufgeräumt hinterlassen, insbesondere keine Dokumente, Geräte, Datenträger mit schützenswerten Inhalten zurücklassen
- Dokumente aus Multifunktions-/Kopiergeräten direkt entnehmen
- Nicht mehr benötigte Dokumente fachgerecht entsorgen (Schredder)
- Laptops und andere mobile Geräte nach Dienstschluss fest- oder einschließen
- Schränke und Schreibtische mit schützenswerten Unterlagen abschließen
- Schlüssel von Türen, Schränken, Schreibtischen sowie Zugangskarten sicher aufbewahren und Verlust unverzüglich melden

Risiko für IT-Sicherheits- und Datenschutzvorfälle im Home Office reduzieren

■ Mobile Arbeit / Telearbeit per VPN



The screenshot shows a web browser window displaying the SCC OpenVPN service page. The page header includes the KIT logo and the text 'Steinbuch Centre for Computing (SCC)'. The main content area is titled 'OpenVPN' and contains the following sections:

- Wichtige aktuelle Meldungen zu OpenVPN**
 - Bitte beachten Sie unsere Hinweise zu macOS und VPNZVLAN.
 - Bitte beachten Sie unsere Hinweise zu älteren OpenVPN-Client-Versionen.
- Aktuelle Information (Nutzung von Split-VPN)**

Der VPN-Zugang erfährt derzeit eine intensive Nutzung aus den Heimnetzen von Beschäftigten und Studierenden des KIT. Wer in einer solch sicheren Umgebung arbeitet, dem empfehlen wir, die **Split-Konfiguration** für sein Betriebssystem herunterzuladen.
- Virtual Private Network**
 - Default:** A diagram showing a user connected to a VPN server, which then connects to internal services.
 - Split tunneling:** A diagram showing a user connected to a VPN server, which connects to internal services, while other traffic goes directly to the internet.

Anleitungen für diverse Betriebssysteme beim SCC:

<http://www.scc.kit.edu/dienste/openvpn.php>

■ Keine Entsorgung von Unterlagen mit sensiblen Informationen im privaten Hausmüll (stattdessen ins Institut mitbringen und schreddern)

Meldepflicht bei IT-Sicherheitsvorfällen

- An ITB und/oder cert@kit.edu
- Ggf. cc an Vorgesetzten

<https://s.kit.edu/it-sicherheit.meldepflicht>



Meldepflichtige IT-Sicherheitsvorfälle

Gemeinsam die KIT IT-Infrastruktur schützen



Verlust von Geräten (z. B. PCs, Laptops, Smartphones), über die Sie auf Dienste oder Daten des KIT zugreifen.



Verlust von Datenträgern (z. B. USB-Sticks, CDs), auf denen vertrauliche Daten wie Passwörter, Klausuren, Bewerbungen, Noten, Gehaltsabrechnungen, Forschungsergebnisse, Erfindungen gespeichert sind.



Entdecken von Geräten, z. B. WLAN-Routern, kleinen Boxen, anderen PCs/Laptops in den eigenen Räumen, die plötzlich da sind, aber nicht angekündigt wurden.



Erpressung oder Nötigung, sich nicht regelkonform zu verhalten, z. B. wenn jemand Unbekanntes unbedingt Zugriff auf Ihre Geräte oder Ihre Räume haben möchte.



Identitätsdiebstahl, nachdem Sie z. B. versehentlich auf einer Phishing-Webseite oder am Telefon ein Passwort preisgeben haben.



Schadsoftware auf Geräten (z. B. PCs, Laptops, Smartphones), über die Sie auf Dienste oder Daten des KIT zugreifen, wird erkannt.

Melden Sie **IT-Sicherheitsvorfälle** bitte umgehend an Ihren lokalen IT-Beauftragten und/oder schicken Sie eine E-Mail an das KIT-CERT: cert@kit.edu. Gemeinsam mit Ihnen wird dann die Situation analysiert und besprochen, was getan werden kann, um das Risiko für das KIT und Sie so gering wie möglich zu halten.

Falls Sie den **Versuch eines Angriffs** feststellen, können Sie diesen Ihrem IT-Beauftragten melden. Falls Sie **unsicher sind**, ob etwas potentiell auf einen Angriff hinweist, fragen Sie gerne bei Ihrem IT-Beauftragten nach und/oder wenden Sie sich an das SCC: beratung-itsec@scc.kit.edu

Ausführliche Informationen zur Meldepflicht von IT-Sicherheitsvorfällen finden Sie unter <https://s.kit.edu/it-sicherheit.meldepflicht>

Die Unterlagen sind urheberrechtlich geschützt.
© KIT 23/08/2019



Informations-
sicherheits-
beauftragter



Meldepflicht bei Datenschutzvorfällen

- Über OE-Leitung über Online-Meldeformular <https://dsb.kit.edu/datenpanne>
- Vorfälle (bezogen auf personenbezogene Daten)
 - Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig
 - Unbefugte Offenlegung/ unbefugter Zugang/ Zugriff
- Beispiele https://www.dsb.kit.edu/downloads/1.Information%20zur%20Meldung%20der%20Datenpannen%20gem.%20Art.%2033%2034%20DS-GVO_20190212.pdf
 - Ein unverschlüsselter Datenträger (USB-Stick oder Festplatte) wird bei einem Einbruch entwendet
 - Personenbezogene Daten einer großen Anzahl Studierender werden versehentlich an eine falsche Mailing-Liste mit mehr als 1.000 Empfängern gesandt
 - Bei einer Mailing-Aktion werden alle Empfänger im „An“- oder „CC“-Feld eingetragen, wodurch alle Empfänger die Adressen der anderen Empfänger sehen können
 - Versand eines Exmatrikulationsbescheides an eine falsche Adresse
 - Bewerbungsmappe ist nicht mehr auffindbar

Datensicherheit (BackUps)

Daten/ Informationen von Geräten zuverlässig an unabhängiger Stelle speichern, um im Fall von

- Befall eines Geräts mit Schadsoftware
- Verlust eines Geräts
- Fehlfunktionen eines Geräts
- versehentliches Löschen

... auf die Daten/ Informationen zugreifen zu können

- Datensicherungsdienst des SCC <https://www.scc.kit.edu/scc/sw/backup/insync/anmeldung/backup.php>
 - PC/Laptop der Sekretariate: ITBs empfehlen nur auf Netzlaufwerk zu speichern
 - Sonstige Geräte: Jeder selbst verantwortlich
- Eigene Lösung → Vorsicht mit Datenschutzanforderungen

Informationssicherheit und Datenschutz

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)
FORSCHUNGSGRUPPE SECURITY · USABILITY · SOCIETY (SECUSO)