Karlsruher Institut für Technologie

Praxistipps IT-Sicherheit am KIT

Gemeinsam die KIT IT-Infrastruktur schützen

Scientific Computing Center

GEMEINSAM DIE KIT IT-INFRASTRUKTUR SCHÜTZEN.

In der Arbeitswelt des KIT ist die IT nicht wegzudenken. Das SCC ist bemüht, mit technischen Maßnahmen die KIT IT-Infrastruktur (hierzu zählen z.B. alle PCs, Laptops, Tablets, Smartphones, Server, WLAN-Router) vor Angriffen zu schützen. Ein effektiver Schutz ist aber nur möglich, wenn alle mithelfen.
Dies ist u.a. im IT-Sicherheitskonzept des KIT geregelt:
https://s.kit.edu/it-sicherheitskonzept

In diesem Faltblatt finden Sie wichtige Hinweise und Tipps zum Schutz der KIT IT-Infrastruktur, sowie Verweise zu weiterführenden Informationen.

Falls Sie Fragen zu den Inhalten des Faltblattes oder darüber hinaus zum Schutz vor Cyberangriffen auf das KIT haben, schicken sie eine Anfrage an
servicedesk@scc.kit.edu

BETRÜGERISCHE NACHRICHTEN ERKENNEN

Kriminelle nutzen verschiedene Strategien, um Unternehmen und Universitäten, und damit auch dem KIT, zu schaden. Eine beliebte Strategie ist das Verschicken von betrügerischen Nachrichten mit dem Ziel

- der Verbreitung von Schadsoftware, um z.B. Zugriffe auf Ihre Geräte und im nächsten Schritt auf die KIT IT-Infrastruktur zu bekommen oder
- des Täuschens der Endanwender, um an sensible Informationen zu gelangen (z.B. an Zugangsdaten) oder sich direkt an Ihnen oder dem KIT monetär zu bereichern.

Die Nachrichten gaukeln Ihnen in der Regel einen legitimen Grund für die Nachricht an Sie vor. Wenn betrügerische Nachrichten es zum Ziel haben, sensible Informationen abzugreifen, dann nennt man diese Nachrichten Phishing-Nachrichten. Da nicht alle betrügerische Nachrichten von den Tools des SCC identifiziert und entfernt werden, ist es wichtig, dass Sie wissen wie Sie betrügerische Nachrichten erkennen. Dies erklären wir Ihnen in einem separaten Faltblatt. Dieses finden Sie unter
https://s.kit.edu/it-sicherheit.betrueg-nachrichten

Wenn Sie zukünftig eine betrügerische Nachricht klar als solche erkennen, dann löschen Sie diese Nachricht unmittelbar. Sie können sich auch beim Meldeverfahren von betrügerischen E-Mails anmelden und betrügerische E-Mails in den entsprechenden Ordner in Ihrem E-Mail-Postfach verschieben. Auch hierdurch helfen Sie, die KIT IT-Infrastruktur zu schützen.

Mehr Informationen zum Meldeverfahren von betrügerischen Nachrichten finden Sie unter:
https://s.kit.edu/it-sicherheit.meldeverfahren

SICHERE PASSWÖRTER

Leider bleiben viele der eingesetzten Schutzmaßnahmen wirkungslos, wenn die Passwörter nicht ausreichend sicher sind. Wer Ihr Passwort kennt oder erraten kann, hat Zugang zu Ihren Daten und kann z.B. auch in Ihrem Namen E-Mails versenden oder auf Ihre Dokumente zugreifen.

Hier finden Sie Hinweise zur Wahl eines sicheren Passwortes und zum Umgang mit Passwörtern:

- Verwenden Sie ein möglichst langes Passwort, d.h. mindestens 12 Zeichen.
- Verwenden Sie für jedes Konto ein einzigartiges Passwort.
- Verwenden Sie für verschiedene Benutzerkonten unterschiedliche Passworte. Falls Sie mehr Benutzerkonten am KIT haben als Sie sich Passworte merken können, nutzen Sie einen Passwort-Manager.
- Halten Sie Ihre Passworte unbedingt geheim. Geben Sie diese auch gegenüber Vorgesetzten, Sekretariaten, IT-Beauftragten, Service-Mitarbeitern, aber auch gegenüber Kollegen, Freunden, Angehörigen oder Partnern nicht preis. Achten Sie bei der Eingabe des Passworts darauf, dass Ihnen niemand über die Schulter schaut.
- Bei Verdacht auf Bekanntsein Ihres Passwortes, ändern Sie es unmittelbar.

VERSCHLÜSSELTE UND SIGNIERTE E-MAILS

E-Mails können von Kriminellen auf dem Weg vom Absender zum Empfänger gelesen oder sogar verändert werden. Damit dies nicht möglich ist und Sie sicher wissen, wer der Absender einer E-Mail ist, sollten Sie Ihre E-Mails verschlüsseln und signieren (so können Sie z.B. auch betrügerische Nachrichten einfacher erkennen). Dies können Sie tun, sobald Sie ein vom KIT ausgestelltes Nutzerzertifikat haben. E-Mails sollten Sie insbesondere dann verschlüsseln, wenn personenbezogene oder andere schützenswerte Daten verschickt werden. Falls Sie noch kein Nutzerzertifikat besitzen, wenden Sie sich bitte an Ihren IT-Beauftragten.

ANTIVIRENSOFTWARE

Die Verwendung von Antivirensoftware ist ebenfalls ein wesentlicher Schutzmechanismus. Das SCC stellt dafür einen zentral verwalteten Antivirendienst zur Verfügung. Wenn bei Ihnen der Antivirendienst noch nicht eingerichtet ist, wenden Sie sich bitte an Ihren IT-Beauftragten.

SICHERER ARBEITSPLATZ

An Ihrem Arbeitsplatz sollen Unbefugten keine schützenswerten Informationen offenbar werden.

Hier finden Sie Regeln und Tipps, was Sie diesbezüglich beachten sollten:

- Schließen Sie Räume immer ab, wenn Sie sie verlassen.
- Schließen Sie die Fenster des Büros, wenn Sie es verlassen, so dass kein Einstieg möglich ist.
- Sperren Sie den Bildschirm oder melden Sie sich ab, wenn Sie Ihren Arbeitsplatz verlassen.
- Aktivieren Sie den Bildschirmschoner mit Passwortschutz und stellen Sie ihn so ein, dass er das Gerät spätestens nach 15 Minuten Wartezeit sperrt.
- Verschlüsseln Sie Notebooks und andere mobile Geräte.
- Schließen Sie Notebooks und andere mobile Geräte nach Dienstschluss fest oder schließen Sie diese ein.
- Schließen Sie Schränke und Schreibtische mit sensiblen Unterlagen ab.
- Bewahren Sie Schlüssel von Schreibtischen und Schränken sicher auf.

BEWUSSTER UMGANG MIT INFORMATIONEN UND DATEN

Seien Sie im Umgang mit schützenswerten Informationen immer besonders aufmerksam. Diese können genutzt werden, um sehr gezielte Angriffe gegen Sie oder das KIT durchzuführen. Daher sollten Sie:

- Solche Informationen nur bewusst und sparsam an Externe geben.
- Verteilerkreise klein halten.
- Unterlagen nur so lange wie nötig aufbewahren.
- Nicht mehr benötigte Datenträger wie Papier, CDs oder DVDs sachgerecht vernichten.
- Nicht mehr benötigte Daten auf mobilen Geräten (Notebook, PDA, Handy, USB-Sticks und dergleichen) löschen. Denken Sie auch daran, Datenträger bei der Außerbetriebnahme zu löschen.

DATENSICHERUNG (BACKUPS)

Wichtige Daten sollen zuverlässig gesichert werden. Mit den Datensicherungsdiensten des SCC können Sie eine Sicherungskopie Ihrer Daten erstellen, so dass diese im Falle eines versehentlichen Löschens, Hardwaredefektes oder eines Angriffs (z.B. durch Schadsoftware) wiederhergestellt werden können. Sprechen Sie Ihren IT-Beauftragten an.
Weitere Informationen:
https://www.scc.kit.edu/dienste/datensicherung

PATCH MANAGEMENT (UPDATES)

Das Versorgen der Geräte und Systeme mit Sicherheitsupdates ist ein wesentlicher Schutzmechanismus. In der Regel werden zeitnah Reparaturen (sog. »Patches«) für bekannte (Sicherheits-) Probleme bereitgestellt. Um das Risiko an Ihren Geräten zu minimieren, ist es wichtig, Updates zeitnah und – wenn möglich – automatisiert einzuspielen. An folgender Stelle finden Sie Anleitungen für die gängigsten Betriebssysteme:
https://www.scc.kit.edu/dienste/patchmanagement

VERWENDUNG VON CLOUD-/ONLINE-DIENSTEN

Bei der Nutzung von Online- oder Cloud-Datendiensten gilt es zu entscheiden, ob Ihre Daten bei diesen Diensten abgelegt werden dürfen. Für die bekanntesten Dienste steht eine Entscheidungshilfe zur Verfügung, mit der Sie dies beurteilen und gegebenenfalls auf eine der angegebenen Alternativen ausweichen können. Die Entscheidungshilfe finden Sie unter:
https://www.scc.kit.edu/dienste/clouddienste

MELDEPFLICHT VON IT-SICHERHEITSVORFÄLLEN

IT-Sicherheitsvorfälle sind zeitnah zu melden.
Eine Meldepflicht besteht für folgende IT-Sicherheitsvorfälle:

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

Melden Sie IT-Sicherheitsvorfälle bitte umgehend an Ihren IT-Beauftragen oder schicken Sie eine E-Mail an **cert@kit.edu**. Gemeinsam mit Ihnen analysieren und besprechen wir, was getan werden kann, um das Risiko so gering wie möglich zu halten.

Weitere Informationen finden Sie unter
https://s.kit.edu/it-sicherheit.meldepflicht

Kontakt
Karlsruher Institut für Technologie (KIT)
Scientific Computing Center (SCC)
ServiceDesk
76131 Karlsruhe, Germany
Tel.: +49 721 608-8000
E-Mail: servicedesk@scc.kit.edu
www.scc.kit.edu

Herausgegeben von
Karlsruher Institut für Technologie (KIT)
Präsident Prof. Dr. Jan S. Hesthaven
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu