Karlsruher Institut für Technologie

E-Mail-Sicherheit

Spam, Phishing und Schadsoftware

IT-SICHERHEIT

Das Wichtigste in Kürze

In dieser Broschüre behandeln wir drei Arten schädlicher E-Mail:

- **Spam** ist ungefragt erhaltene E-Mail mit Werbemüll oder sonstigem wertlosen Inhalt. Der primäre Schaden besteht in der verlorenen Arbeitszeit.
- Mit **Phishing** wird versucht, Sie zur Herausgabe sensibler Daten wie beispielsweise Ihrer KIT-Zugangsdaten zu bewegen.
- E-Mail mit **Schadsoftware** als Anhang oder Link.

Sie haben Spam empfangen?

- Sie können Spam einfach **ignorieren** und **löschen**. Je weniger Zeit Sie auf diese E-Mails verwenden, desto besser.
- Sie können diese E-Mails auch dem SCC melden. Damit helfen Sie mit, die zentralen Spamfilter zu verbessern. Weitere Informationen zur Teilnahme am **Spam-Meldeverfahren** finden Sie hier:

https://www.scc.kit.edu/sl/spam

In Ihrem Namen wird Spam versendet?

Sie erhalten massenhaft Rückläufer-Mails, die suggerieren, über Ihr KIT-Konto würde Spam verschickt? Glücklicherweise ist das meistens nicht der Fall: Um Spamfilter zu umgehen, versenden Angreifer Spam mit gefälschten, aber realen Absenderadressen. Wie bei Briefpost ist das nicht zu verhindern.

Meist hält eine solche Welle von Rückläufern nur wenige Stunden an – es genügt, wenn Sie einfach abwarten.

Sie möchten sich besser wappnen?

- Halten Sie immer Betriebssystem und Anwendungen aktuell. Spielen Sie alle Sicherheitsupdates zeitnah ein.
- Verbieten Sie die Ausführung von Makros in Office-Dokumenten.
- Sorgen Sie für adäquaten Virenschutz. Das KIT hat ein entsprechendes Angebot:

https://www.scc.kit.edu/sl/viren

Sind Sie einem Betrugsversuch zum Opfer gefallen?

- Haben Sie Ihr Passwort per E-Mail oder im Web weitergegeben?
- Haben Sie einen E-Mail-Anhang geöffnet, der Ihnen merkwürdig vorkommt?
- Sind Sie einem Link gefolgt, der unerwartete Inhalte liefert, Sie überraschend zur Preisgabe von Daten oder zu einem Download auffordert?

Dies sind mögliche Merkmale eines Angriffs. Sprechen Sie im Zweifel mit Ihrem IT-Beauftragten. Kontaktieren Sie bei konkretem Verdacht das KIT-CERT, das Ihnen bei IT-Sicherheitsvorfällen hilft.

Schädliche E-Mails: Gefahr für das KIT

Das KIT steht als Wissenschaftseinrichtung in einer besonderen Situation – wir wirken einerseits in der Öffentlichkeit und müssen andererseits Informationen vor Dritten schützen. Für Sie als Mitarbeiter ist Kommunikation, insbesondere über E-Mail, unerlässlich für Ihre Arbeit. E-Mail ist deshalb ein häufig genutztes Einfallstor für Angreifer.

Angreifer möchten Zugriff auf Ihre Daten und IT-Systeme erlangen und versuchen deshalb, Sie zum Öffnen schädlicher Anhänge oder Weblinks zu verleiten.

Technisch kann man die Angriffe nicht vollständig verhindern, ohne Sie in Ihrer Arbeitsfähigkeit stark zu beeinträchtigen. **Sensibles Verhalten** ist daher ein wichtiger Teil des gesamten IT-Sicherheitsprozesses am KIT.

Diese Broschüre gibt Ihnen auch hierfür die wichtigsten Informationen.

Sie empfangen schädliche E-Mails?

- Sie können schädliche E-Mails jeglicher Art **ignorieren** und **löschen**. Dies ist die einfachste und schnellste Methode, damit umzugehen.
- Eingehende E-Mails werden automatisch auf Spam untersucht und entsprechend markiert. Spam wird dann in einen separaten Mailordner verschoben, wenn Sie diesen Dienst aktiviert haben.
- Gelegentlich wird Spam nicht erkannt. Sie können uns helfen, die Erkennung zu verbessern, indem Sie solche E-Mails in den **Spam-Meldeordner** verschieben. Der Spamfilter wird dann mit diesen E-Mails trainiert.

Wie erkennen Sie Phishing oder E-Mails mit Schadsoftware?

Bei **Phishing** wird versucht, Ihnen einen legitimen Zweck vorzugaukeln, um Sie zur Herausgabe schützenswerter Daten – wie beispielsweise Ihres Passworts – zu bewegen.

Bei **Malware-Angriffen** wird versucht, Schadsoftware auf Ihrem Computer auszuführen. Das ermöglicht eine Vielzahl weiterer Angriffe wie beispielsweise das Nachladen von Verschlüsselungstrojanern.

Ein guter Angriff ist sehr schwer erkennbar. Mit den folgenden Fragen können Sie sich an eine Entscheidung herantasten:

- Erhalten Sie die E-Mail unerwartet?
- Ist die Anrede falsch oder passt sie nicht zur Empfängeradresse?
- Haben Sie noch niemals mit dem Absender kommuniziert?
- Werden Sie um die Herausgabe vertraulicher Daten gebeten?
- Versucht der Absender, Druck auf Sie auszuüben? »Wenn Sie nicht sofort reagieren, sperren wir Ihr Konto!«, »Ihr Computer ist gefährdet…«
- Führen die in der E-Mail enthaltenen Links auf andere Seiten als beschrieben? Hinweis: Ihr E-Mail-Programm kann Ihnen Ziele von Links anzeigen, ohne diese zu öffnen.
- Ist das Anliegen sehr allgemein gehalten oder aber detailliert und Ihnen völlig unbekannt?
- Sind Anhänge enthalten, die unspezifische Namen tragen wie »Rechnung-2752.zip« oder »Invoice.exe«?
- Passt das Anliegen nicht zu Ihrem KIT-Kontext?
- Hätten Sie Hemmungen, die Informationen herauszugeben, wenn Sie ein Fremder an Ihrer Haustür danach fragen würde?
- Ist die E-Mail von einem KIT-Absender und nicht digital signiert?

Je mehr Fragen Sie mit »ja« beantworten, desto eher handelt es sich um eine schädliche E-Mail.

Halten Sie im Zweifel auf anderem Weg Rücksprache mit dem angeblichen Absender.

Übrigens: Diese Prüffragen sind auch anwendbar auf Telefon, Fax und Briefpost.

Wie können Sie sich schützen?

Sie können sich vor schädlicher E-Mail besser schützen, indem Sie das Folgende beachten:

- Wenn Sie eine E-Mail für schädlich halten, ignorieren und löschen Sie sie.
- Wenn Sie sich unsicher sind, setzen Sie sich mit dem vermeintlichen Absender in Verbindung.
- Das SCC fordert Sie **niemals** dazu auf, Ihr Passwort offenzulegen. Sollte Sie jemand dazu auffordern, handelt es sich um einen Sicherheitsvorfall, über den Sie das KIT-CERT unverzüglich informieren sollten! Die Kontaktinformationen des KIT-CERT finden Sie auf der Rückseite dieses Flyers.
- Halten Sie Betriebssystem und Anwendungen auf Ihrem Rechner stets auf dem aktuellen Patchstand. Auf diese Weise minimieren Sie die Angriffsfläche Ihres Systems.

https://www.scc.kit.edu/sl/patch

- Sorgen Sie für adäquaten Virenschutz und halten Sie ihn aktuell. Das Angebot des SCC finden Sie hier:

https://www.scc.kit.edu/sl/viren

- Sie helfen uns, die Mailfilter zu verbessern, indem Sie aktiv am Spam-Meldeverfahren teilnehmen.

https://www.scc.kit.edu/sl/spam

- Bei einem konkreten Angriffsverdacht kontaktieren Sie bitte das KIT-CERT.

Was tun im Schadensfall?

Gut gemachte Angriffe sind sehr schwer als solche zu erkennen. Daher kann es vorkommen, dass schützenswerte Daten und Systeme in falsche Hände geraten.

Wenn Sie vermuten, dass dies bei Ihnen der Fall ist, setzen Sie sich umgehend mit Ihrem IT-Beauftragten und dem KIT-CERT in Verbindung. Das KIT-CERT unterstützt Sie bei der Koordination und Bewältigung von IT-Sicherheitsvorfällen. Nur so kann weiterer Schaden von Ihren Daten und der IT-Infrastruktur des KIT abgewendet werden.

KIT CERT

Kontakt

KIT Computer Emergency Response Team (KIT-CERT)

Telefon: +49 721 608-45678
E-Mail: cert@kit.edu

www.cert.kit.edu

Herausgeber

Karlsruher Institut für Technologie (KIT)
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

Stand: 2019-05-06 (Revision 22/cc6df56)