Allgemeine Informationen

Kriminelle nutzen verschiedene Strategien, um Unternehmen und Universitäten und damit auch dem KIT zu schaden. Beliebte Angriffsstrategien sind

- die Verbreitung von Schadsoftware, um z. B. Zugriff auf Ihre Geräte und im nächsten Schritt auf die KIT IT-Infrastruktur zu bekommen oder
- das Täuschen der Endanwender, um an sensible Informationen zu gelangen (z. B. an Zugangsdaten).

Eine weit verbreitete Angriffsmethode ist es, Ihnen betrügerische Nachrichten zu schicken, die Ihnen einen legitimen Grund für die Nachricht an Sie vorgaukeln. Betrügerische Nachrichten können Sie über unterschiedliche Kanäle empfangen, z. B. als E-Mail, SMS, Nachricht über Messenger bzw. soziale Netzwerke. Für KIT-Mitarbeiter*innen ist die Gefahr im Kontext von E-Mails am größten, da oft die Namen auf der Webseite stehen und so die E-Mail-Adresse einfach ermittelt werden kann.

Die Inhalte dieser Nachrichten können auf unterschiedliche Art und Weise gefährlich sein:

Sensible Daten: Nachrichten fordern Sie auf, sensible Daten wie Zugangsdaten oder schützenswerte Dokumente zurückzuschicken.

Überweisungen/Anrufe: Nachrichten fordern Sie auf, Überweisungen oder Anrufe, z. B. an Kooperationspartner, vermeintliche Freunde oder Geschäftspartner, zu tätigen. So erhalten die Kriminellen eine direkte Überweisung von Ihnen oder der Betrag wird über die Telefonrechnung abgebucht.

Links: Nachrichten können einen oder mehrere gefährliche Links enthalten (diese Form betrügerischer Nachrichten wird auch als Phishing-Nachricht bezeichnet). Ziel des Betrugs ist es, dass Sie auf einen der Links klicken. Diese Links leiten Sie dann z. B. zu einer echt aussehenden, aber betrügerischen Webseite (auch als Phishing-Seite bezeichnet), bei der Sie sich einloggen sollen. Alternativ werden Sie zu einer Webseite weitergeleitet, die Ihnen auf Ihrem Gerät Schadsoftware installiert.

Anhänge: Nachrichten enthalten eine oder mehrere gefährliche Dateien (wie z. B. einen Anhang in einer E-Mail). Ziel der Kriminellen ist es, dass Sie den Anhang öffnen. Durch das Öffnen bzw. Ausführen der Datei wird auf Ihrem Gerät Schadsoftware installiert.

Werbung: Nachrichten enthalten Werbung oder sonstige wertlose Inhalte (diese Nachrichten werden häufig als Spam bezeichnet). Ziel des Angriffs ist es, dass Sie etwas kaufen. Der primäre Schaden ist in der Realität jedoch die verlorene Arbeitszeit, weil Sie die Nachricht kurz ansehen, bewerten und dann löschen.

Gemeinsam die KIT IT-Infrastruktur schützen

Das Steinbuch Centre for Computing (SCC) setzt technische Maßnahmen ein, um betrügerische Nachrichten, die ins KIT-Netz gelangen, automatisiert zu erkennen. Diese werden Ihnen erst gar nicht zugestellt. Leider ist es mit den existierenden Tools nicht möglich, alle betrügerischen Nachrichten zu entdecken, da einerseits betrügerische Nachrichten immer schwerer zu entdecken sind, da die Angriffsmethoden immer besser werden, und da andererseits dem SCC daran gelegen ist, Sie nicht durch zu strikte Regeln bei Ihrer Arbeit zu behindern. Zu strikte Regeln hätten die Konsequenz, dass auch Nachrichten nicht zugestellt werden, die gar nicht betrügerisch sind, aber zufällig ähnliche Eigenschaften wie betrügerische Nachrichten aufzeigen.

Daher ist es wichtig, dass Sie bei der Entdeckung von betrügerischen Nachrichten mithelfen. Ihre Unterstützung ist ein wichtiger Bestandteil des gesamten IT-Sicherheitskonzepts am KIT.

In diesem Faltblatt finden Sie sowohl allgemeine Informationen über betrügerische Nachrichten, als auch sieben Regeln, wie Sie betrügerische Nachrichten erkennen.

Mit Hilfe dieser Regeln werden Sie die meisten betrügerischen Nachrichten erkennen können. Im Alltag liegt Ihr Fokus nicht immer auf der Prüfung von Nachrichten. Wenn Sie daher doch mal auf eine betrügerische Nachricht reinfallen und es anschließend merken, **melden Sie sich umgehend bei Ihren lokalen IT-Beauftragten oder schicken Sie eine E-Mail an cert@kit.edu**. Bitte haben Sie dabei keine Angst. Auch mit dem (schnellen) Melden von Vorkommnissen tragen Sie dazu bei, das KIT vor erfolgreichen Angriffen zu schützen und/oder das Ausmaß des Schadens so gering wie möglich zu halten.

Wenn Sie zukünftig eine betrügerische Nachricht klar als solche erkennen, dann löschen Sie diese Nachricht unmittelbar. Wenn Sie sich beim Meldeverfahren von betrügerischen E-Mails angemeldet haben, verschieben Sie die betrügerische E-Mail in den entsprechenden Ordner in Ihrem E-Mail-Postfach. 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

Wenn Sie eine Nachricht erhalten, bei der Sie sich unsicher sind, ob diese eine betrügerische Nachricht ist, dann kontaktieren Sie Ihre lokalen IT-Beauftragten oder schicken Sie die E-Mail an beratung-itsec@scc.kit.edu weiter, mit der Bitte, Ihnen bei der Entscheidung, ob es sich hierbei um eine betrügerische Nachricht handelt, zu helfen.

Kontakt

Steinbruch Centre for Computing (SCC)
Abteilung IT-Security und Service-Management
(ISM) Andreas Lorenz

Telefon: +49 721 608 245 00
E-Mail: beratung-itsec@scc.kit.edu

https://www.scc.kit.edu

Digital Office
Informationssicherheitsbeauftragter
Milan Burgdorf

Telefon: +49 721 608 - 41035
E-Mail: informationssicherheitsbeauftragter@kit.edu

https://www.digitaloffice.kit.edu

Competence Center for Applied Security Technology (KASTEL)
Institut für Angewandte Informatik
und Formale Beschreibungsverfahren (AIFB)
Forschungsgruppe Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Gebäude 05.20
76133 Karlsruhe

Telefon: +49 721 608 450 45
E-Mail: secuso@aifb.kit.edu

https://secuso.aifb.kit.edu
https://twitter.com/secusoresearch

100 % Recyclingpapier mit dem Gütesiegel „Der Blaue Engel"

Herausgeber

Karlsruher Institut für Technologie (KIT)

Präsident Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
https://www.kit.edu

Der Inhalt des Faltblatts basiert auf Erkenntnissen aus dem Projekt „KMU AWARE – Awareness im Mittelstand", welches die Forschungsgruppe SECUSO an der TU Darmstadt durchgeführt hat und welches im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft" vom Bundesministerium für Wirtschaft und Energie bis zum 31.03.2018 gefördert wurde. Die Finanzierung des Faltblatts erfolgt im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts KASTEL.

Karlsruher Institut für Technologie

Betrügerische Nachrichten

Wie Sie betrügerische Nachrichten und insbesondere Phishing-Nachrichten erkennen können

Eine Kooperation von SCC, dem Informationssicherheitsbeauftragten, der Forschungsgruppe SECUSO am AIFB und KASTEL

SCC Steinbuch Centre for Computing · Informationssicherheitsbeauftragter · aifb · KASTEL · SECUSO SECURITY · USABILITY · SOCIETY

Folgende Regeln helfen Ihnen, betrügerische Nachrichten zu erkennen

1. Regel: Prüfen Sie Absender und Inhalt jeder empfangenen Nachricht auf Plausibilität:

- Passt der Absender nicht zur Nachricht?
  - ✗ Der Absender info@sye.jp ist bei einer SECUSO E-Mail nicht plausibel.
  - ✓ Der Absender info@secuso.org ist bei einer SECUSO E-Mail plausibel.
- Werden sensible Daten abgefragt?
- Werden Sie aufgefordert, Geld zu überweisen oder jemanden anzurufen, wobei in der Nachricht die dafür nötigen Informationen angegeben sind?
- Haben Sie dort kein Nutzerkonto?
- Erhalten Sie die Nachricht unerwartet?
- Ist die Anrede falsch oder passt diese nicht zum Absender?
- Im Fall von E-Mails: Ist die E-Mail von der entsprechenden Person nicht digital signiert?

Je mehr Fragen Sie mit „ja" beantworten können, desto wahrscheinlicher handelt es sich um eine betrügerische Nachricht. Besondere Vorsicht ist bei den sensiblen Daten inkl. Passwörtern gefragt. KIT-Stellen inkl. dem SCC und den lokalen IT-Beauftragten würden Sie nicht auffordern, dass Sie ihnen Ihr Passwort zusenden.

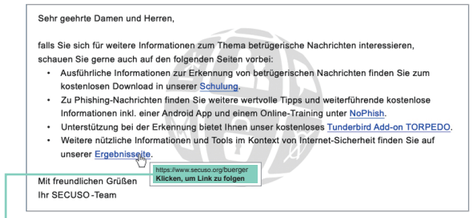
Übrigens: Die meisten der obigen Fragen können Sie auch auf den Telefon-, Fax- bzw. Briefpost-Kontext anwenden.

2. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen oder mehrere Links enthält, prüfen Sie, ob es sich um eine gut gemachte betrügerische Nachricht handelt, d. h. bei der jemand vorgibt, der (vermeintliche) Absender zu sein, bevor Sie voreilig auf einen der Links klicken. Dazu untersuchen Sie den Link.

Ein Link kann meist daran erkannt werden, dass der Text blau und unterstrichen ist. Jedoch können Links auch in Form von Buttons oder Bildern in Nachrichten integriert sein.

Um den Link zu untersuchen, müssen Sie zunächst herausfinden, welche Webadresse (auch URL genannt) tatsächlich hinter dem Link steckt. Diese Information ist je nach Gerät, Software und Dienst (z. B. Amazon, Dropbox, Skype, WhatsApp, Facebook, Google+, Xing, LinkedIn) an unterschiedlichen Stellen zu finden. Sie sollten sich also vor der Nutzung eines Geräts, einer Software bzw. eines Dienstes damit vertraut machen, wo die tatsächliche Webadresse eines Links zu finden ist.

Bei PCs und Laptops erscheinen die Webadressen in der Regel, wenn Sie mit der Maus den Link berühren, ohne ihn anzuklicken. Der Link wird entweder in der Statusleiste am Fuß des Fensters oder in einem Infofeld, welches auch Tooltip genannt wird, erscheinen.

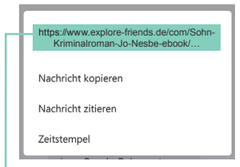


Webadresse im Tooltip (z. B. bei Outlook)

Webadresse in der Statusleiste (z. B. bei Thunderbird oder Webbrowsern wie Firefox, Internet Explorer und Chrome)

Bei mobilen Geräten (Smartphones und Tablets) hängt das Vorgehen zum Identifizieren der Webadresse eines Links stark vom Gerät und von der jeweiligen App ab. Meist ist es so: Wenn Sie Ihren Finger für mindestens 2 Sekunden auf dem Link halten, dann wird die Webadresse im Dialogfenster angezeigt. Achten Sie darauf, dass Sie den Link dabei nicht versehentlich anklicken. Wenn Sie unsicher sind, warten Sie, bis Sie wieder an Ihrem PC oder Laptop sind.

Webadresse im Dialogfenster (Betriebssystem iOS)



Webadresse im Dialogfenster (Betriebssystem Android)

3. Regel: Wenn Sie die Webadresse hinter dem Link gefunden haben, identifizieren Sie als Nächstes den sogenannten Wer-Bereich in der Webadresse.

https://nophish.secuso.org/login

Wer-Bereich

Der Wer-Bereich einer Webadresse besteht aus den beiden Begriffen, die durch einen Punkt getrennt sind und sich vor dem ersten alleinstehenden Schrägstrich „/" befinden (in diesem Fall secuso.org). Der Wer-Bereich ist der wichtigste Bereich (d. h. der wichtigste Indikator) für die Erkennung gefährlicher Webadressen und damit von Nachrichten mit gefährlichen Links. In der Fachsprache wird er „Domain" genannt. Falls hier Zahlen stehen, handelt es sich um eine sogenannte IP-Adresse und es ist höchstwahrscheinlich eine gefährliche Webadresse.

✗ https://www.129.13.152.9/secuso.org.secure-login.de/

4. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, prüfen Sie, ob der Wer-Bereich einen Bezug zu dem (vermeintlichen) Absender und dem Inhalt der Nachricht hat und ob er korrekt geschrieben ist. Wenn Absender oder Betreff nicht zum Inhalt passen, dann klicken Sie nicht auf den Link.

Kriminelle schreiben den zu erwartenden Wer-Bereich an eine andere Stelle in die Webadresse, um Sie zu täuschen: z. B.

✓ https://www.mein-paketservice.de/

✗ https://www.mein-paketservice.de.shoppen-im-web.de/

✗ https://shoppen-im-web.de/mein-paketservice.de/

Kriminelle registrieren Wer-Bereiche (also die entsprechenden Internet-Domains), die mit dem eigentlichen Wer-Bereich bis auf wenige Zeichen übereinstimmen: z. B.

✓ https://www.bauernmarkt-total.de/

✗ https://www.baurenmarkt-total.de/

✗ https://www.bauemmarkt-total.de/

✗ https://www.bauerrnmarkt-total.de/

5.Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, ihn aber nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mittels einer Suche der Adresse in einer Suchmaschine. Wenn Sie danach immer noch unsicher sind, kontaktieren Sie Ihre lokalen IT-Beauftragten bzw. stellen eine Anfrage an beratung-itsec@scc.kit.edu. Gemeinsam mit Ihnen wird die Nachricht dann beurteilt.

✓ https://www.secuso.org/

✗ https://www.secuso-research.org/

6. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Anhang enthält, dann prüfen Sie, ob dieser Anhang ein potenziell (sehr) gefährliches Dateiformat hat. Potenziell gefährliche Dateiformate sind:

- Direkt ausführbare Dateiformate (sehr gefährlich): z. B. .exe, .bat, .com, .cmd, .scr, .pif
- Dateiformate, die Makros enthalten können: z. B. Microsoft Office Dateien wie .doc, .docx, .docm, .ppt, .pptx, .xls, .xlsx
- Dateiformate, die Sie nicht kennen

7. Regel: Wenn das Dateiformat potenziell (sehr) gefährlich ist, dann öffnen Sie den Anhang nur, wenn Sie diesen genauso von dem Absender erwarten. Falls Sie unsicher sind, ob Sie die Nachricht einfach löschen können, sollten Sie weitere Informationen einholen. Dabei verwenden Sie auf keinen Fall die Kontaktmöglichkeiten aus der Nachricht. Rufen Sie z. B. den Absender an.

Wenn Sie bei Office-Programmen nach dem Öffnen gefragt werden, ob sogenannte Makros ausgeführt werden sollen, ist dies ein guter Zeitpunkt, erneut zu überlegen, ob die Nachricht, aus der die Datei stammt, nicht doch eine betrügerische Nachricht ist. Brechen Sie den Vorgang erst einmal ab.

Wenn Sie unsicher sind, dann kontaktieren Sie Ihre lokalen IT-Beauftragten bzw. stellen eine Anfrage an beratung-itsec@scc.kit.edu. Gemeinsam mit Ihnen wird die Nachricht dann beurteilt.

Weitere Informationen

Wie Sie betrügerische Nachrichten mit Links erkennen, wird Ihnen auch anschaulich in zwei Videos erklärt:

Zu den Erklär-Videos
https://s.kit.edu/it-sicherheit.betrueg-nachrichten.videos

Wenn Sie die Informationen zu betrügerischen Nachrichten mit Links aus diesem Faltblatt vertiefen möchten, dann können Sie dies über das NoPhish-Lernmodul bei ILIAS tun:

Zur NoPhish Schulung
https://s.kit.edu/it-sicherheit.betrueg-nachrichten.schulung

Übrigens: Wenn Sie massenhaft Rückmeldung erhalten, dass jemand eine E-Mail von Ihnen erhalten hat, die Sie gar nicht verschickt haben, dann informieren Sie Ihre lokalen IT-Beauftragten. Gemeinsam mit Ihnen wird dann die Situation analysiert und besprochen, was getan werden kann, um das Problem zu beheben.