IT-Sicherheitstipp Nr.3 – Mai 2019

Gefahren durch E-Mails

Übermittlung von E-Mails im Internet

Ähnlich wie bei der Briefpost werden E-Mails im Internet von einem „Briefzentrum“ zum nächsten in Form von Computerservern geschickt und schließlich dem Adressaten zugestellt.

Im Unterschied zur Briefpost gibt es jedoch beim E-Mail-Transport über das Internet keinen allein verantwortlichen Dienstleister, der die Beförderung und Zustellung übernimmt. Die E-Mail wird auf nicht vorhersagbaren Wegen über viele Rechner in unterschiedlichsten Firmen, Behörden und Ländern weitergeleitet.

Risiken der E-Mail-Nutzung:

- Kein einheitlicher Vertragspartner
- Keine Gewährleistung
- Keine Zustellgarantie
- E-Mails sind wie eine kostenlose Postkarte, die jeder lesen – und verändern! – kann
- Können Angriffstechniken wie Phishing, Viren oder Würmer enthalten

Auch der Absender wird nicht überprüft. Überhaupt ist eine E-Mail am ehesten mit einer Postkarte vergleichbar, die von allen möglichen Personen auf ihrem Weg gelesen und sogar verändert werden kann.

Es könnte passieren, dass Sie eine E-Mail mit einer gefälschten Absenderadresse oder veränderten Inhalten bekommen!

So verhalten Sie sich richtig:

- Beantworten Sie keine Spam-E-Mails
- Vermeiden Sie bei unbekannten E-Mails das Klicken auf Links innerhalb des Texts – diese können gefälscht sein
- Geben Sie im Zweifelsfall Links lieber per Hand in die Adresszeile Ihres Browsers ein
- Öffnen Sie keine Anhänge unbekannter Absender
- Löschen Sie Spam-E-Mails aus Ihrem Postfach

Spam-E-Mails und der Schutz davor

E-Mails kosten kein Porto. Das führt zu einem unschönen Problem. Es ist einfach, tausende von E-Mails zu verschicken. Das wird von Firmen für den Versand von Werbe-Mails ausgenutzt, die kostbare Ressourcen belegen und Ihr Postfach füllen. Diese Mails werden auch als Spam-E-Mails, kurz "Spam" oder Junk-Mails bezeichnet.

Ca. 90% der heute empfangenen E-Mails sind Spam. In vielen Verwaltungen werden E-Mails beim Eingang automatisch zentral überprüft. Offensichtliche Spam-E-Mails werden dann entsprechend gekennzeichnet oder automatisch abgewiesen.

Fehlgeleitete Informationen

Immer wieder führt menschliches Fehlverhalten dazu, dass Informationen fehlgeleitet werden und in falsche Hände geraten. Dies kann unter Umständen erhebliche wirtschaftliche und rechtliche Folgen für Sie, Kolleginnen und Kollegen und Ihre Verwaltung haben.

„Erste Hilfe“ bei fehlgeleiteten Informationen

Wie verhalten Sie sich richtig, wenn Sie selbst versehentlich vertrauliche Informationen an Unbefugte gesendet haben?

- Informieren Sie unverzüglich Ihre Vorgesetzten und Ihre/n Datenschutzbeauftragte/n
- Informieren Sie den Empfänger oder die Empfängerin über die fälschlich übermittelte E-Mail und bitten um deren Löschung
- Leiten Sie gemeinsam mit Ihren Vorgesetzten und ggf. dem oder der Datenschutzbeauftragten alle notwendigen Maßnahmen zur Begrenzung des Schadens ein

Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf

und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Geht mich nichts an?
Mit Sicherheit!

Cybersicherheit

Umgang mit vertraulichen Informationen und E-Mail-Verschlüsselung

Wir alle arbeiten heute mit mehr oder weniger vertraulichen Informationen. Gerade bei der Verwendung von E-Mails kann es leicht passieren, dass sensible Daten an die Falschen oder zu viele Empfänger oder Empfängerinnen geschickt werden.

Der unverschlüsselte Versand vertraulicher Informationen über das Internet kommt dem Versand sensibler Daten per Postkarte gleich und ist daher zu unterlassen.

Den Inhalt und Anhänge von E-Mails kann man verschlüsseln, so dass Texte, Fotos etc. nicht lesbar sind. Möglich machen das mathematische Verschlüsselungsverfahren. Sie verändern die Inhalte so, dass nur Berechtigte sie lesen können. Der Empfänger der E-Mail kann sie nach seinem Entschlüsseln öffnen. Die E-Mail ist so auch für die Übermittlungsstellen nicht mehr zu lesen – nur für die berechtigten Empfängerinnen oder Empfänger.

Umgang mit fehlgeleiteten E-Mails:

- Geben Sie die E-Mail und deren Inhalt nicht weiter
- Informieren Sie den Absender oder die Absenderin
- Löschen Sie die E-Mail aus Ihrem Postfach

Phishing und Pharming

Phishing bedeutet Passwortdiebstahl per Internet. Er erfolgt meist per E-Mail. Phishing-E-Mails sind als seriöse Nachricht z.B. einer Bank getarnt und fordern den Empfänger oder die Empfängerin auf, persönliche Daten, Passwörter oder PINs zu aktualisieren. Mit den Daten können die Betrügerinnen und Betrüger dann ungehindert die Konten plündern.

Phishing ist eine der häufigsten Spielarten der Online-Kriminalität. Jeder einzelne Vorstoß kann mehrere Millionen Internetnutzerinnen und -nutzer erreichen.

Beim **Spear-Phishing** wird das Opfer gezielt ausgewählt. Das können auch Sie sein! Alle Hierarchie-Ebenen von der Sachbearbeitung und Assistenz bis zur Behördenleitung stehen im Fokus.

Pharming ist eine Weiterentwicklung des Phishings. Der Angriff besteht darin, eine in den Browser eingegebene Internetadresse unbemerkt auf eine Website des Angreifers umzuleiten.

Die auf Ihrem Rechner zwischengespeicherten Adressen für Internet-Seiten werden dabei durch den Angreifer überschrieben. Obwohl Sie die korrekte Internetadresse eingetippt haben, erfolgt beim Aufruf der Webseite eine automatische Umleitung auf die Seite des Angreifers! Dort lauern dann Viren oder man will Ihre Kontozugangsdaten unberechtigt abfragen.

Schutzmaßnahmen:

- Geben Sie niemals geheime Daten wie Passwörter, Kontodaten oder PIN nach Aufruf eines Links aus einer E-Mail ein
- Passwörter, PIN und TAN sollten Sie nur auf den Original-Servern des Kreditinstituts eingeben – am Besten immer die Internet-Adresse eintippen
- Achten Sie bei der Adresse auf die richtige Schreibweise
- Achtung: Banken fragen Sie niemals nach Ihrem Passwort oder fordern Sie per E-Mail zur Aktualisierung Ihrer persönlichen Daten auf

Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf

und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Geht mich nichts an?
Mit Sicherheit!

Cybersicherheit

So verhalten Sie sich richtig im Behördennetz

- Die Empfängerliste überprüfen, ob eventuell unerwünschte Personen enthalten sind (insbesondere bei Antworten auf eine E-Mail und dem Klicken auf „Allen antworten“).
- Überprüfen, ob die ausgewählten Anlagen, Empfängernamen bzw. E-Mail-Adressen korrekt sind.

So verhalten Sie sich richtig im Internet

- Vertrauliche Daten sollten nur in Ausnahmefällen an externe Personen per E-Mail geschickt werden.
- Vertrauliche Daten dürfen nicht unverschlüsselt über unsichere Wege verschickt werden – dazu gehört gerade das Internet!
- Sollten Sie keine E-Mail-Verschlüsselung durchführen können, müssen vertrauliche Daten über die üblichen alternativen, meist papiergebundenen Wege übermittelt werden.

So verhalten Sie sich richtig bei unseriösen Nachrichten

- Nicht voreilig handeln. Klicken Sie erstmal keine Links an und öffnen Sie keine Anhänge.
- Fragen Sie beim Absender nach (am besten telefonisch) und versichern Sie sich, dass dieser Ihnen wirklich diese E-Mail gesendet hat.
- Ist diese E-Mail nicht von ihm, löschen Sie diese E-Mail sofort! Lieber einmal zu viel löschen als einmal zu wenig. Wichtige Nachrichten können nochmals zugestellt werden.

So verhalten Sie sich richtig im Notfall

- Sofort den Computer herunterfahren und den Stromstecker ziehen, um einen weiteren Schaden zu vermeiden.
- Umgehend Ihre Kolleginnen oder Kollegen der IT-Abteilung informieren.
- Auf eine Rückmeldung warten.

Machen Sie den Test. Sind folgende Nachrichten vertrauenswürdig?

Mit der Lupe oder dem Zoom Ihres PDF-Programms können Sie die Bilder vergrößern und genau betrachten.
Über die Kamera Ihres Smartphones können Sie die Antwortmöglichkeit einscannen. Auf der hinterlegten Webseite finden Sie die richtige Antwort sowie einige weitere Hintergrundinformationen.

Vielen Dank an die Forschungsgruppe SECUSO des Instituts für Angewandte Informatik und Formale Beschreibungssprachen des Karlsruher Instituts für Technologie (KIT) für die Bereitstellung des Materials.