Leitfaden zum sicheren Umgang mit eMails:

Worauf Sie achten sollten und wie Sie verdächtige Nachrichten erkennen

Auf diesen Seiten finden Sie Hinweise und Tipps zur Nutzung von eMail.

Die Informationen gliedern sich dabei in drei Bereiche:

- **Teil I: Versenden von eMails**
- **Teil II: Der Empfang von eMails**
- **Teil III: Informationen zu Dateitypen und Erweiterungen**

Mit freundlicher Genehmigung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), http://www.datenschutzzentrum.de

Teil I: Versenden von eMails:

1. Der Betreff

- Verwenden Sie **immer** eine **Betreffzeile**.
- Der Betreff sollte **kurz** und **aussagekräftig** sein, idealerweise den Inhalt der Nachricht bzw. die Thematik kurz umreißen.

Warum?

Zum einen erleichtert eine kurze, klare Betreffzeile dem Empfänger die Abarbeitung der Mail - er kann schnell entscheiden, in welchen Kontext diese gehört, und kann sie entsprechend bearbeiten.

Zum anderen wird durch eine aussagekräftige Betreffzeile deutlich, dass es sich nicht um eine automatisch generierte Nachricht eines Mailwurms handelt. Diese verwenden häufig nur pauschale Betreffzeilen wie "Hi!" oder "Ihre Anfrage".

2. Der Text

- Verwenden Sie **immer** eine **direkte Ansprache** des Empfängers.
- **Erwähnen** Sie **immer** eventuell beigefügte **Anhänge** (Attachments): "Anbei übersende ich Ihnen...." oder "Hier die Ergebnisse der ..."

Warum?

Auch die direkte Anrede macht klar, dass die Nachricht nicht von einem Mailwurm stammt.

Anhänge, die Sie einer Mail beifügen, sollten Sie als solche auch kenntlich machen. Andernfalls könnte der Verdacht entstehen, der Anhang sei durch einen Wurm erzeugt und der Mail automatisch beigefügt.

3. Der Anhang

- **Vermeiden Sie Anhänge, wenn es geht** . Einfache Texte ohne Formatierungen können ebenso gut direkt in die Mail kopiert werden!
- Versenden Sie **nur potentiell sichere Dokumenttypen** . (Mehr dazu in Teil III dieses Textes)
- Versenden Sie Word-Dokumente nur im Ausnahmefall und nur auf ausdrücklichen Wunsch des Empfängers!

Warum?

Durch die Vermeidung eines Anhangs ersparen Sie dem Empfänger nicht nur Zeit (er muss kein separates Programm zum Betrachten starten), sondern auch die Mühe zu entscheiden, ob er Ihrem Anhang traut und ihn öffnet.

Durch das Verwenden potentiell sicherer Formate wie PDF setzen Sie ein **klares Zeichen für den Empfänger** : Diese Mail enthält keinen Wurm oder Virus.

Bei Word-Dokumenten gilt **besondere Vorsicht** . Dabei sind eventuell enthaltene Makroviren nur die eine Gefahr. Ein anderes Risiko stellen in Word-Dokumenten enthaltene Revisionsinformationen dar. Das können die letzten Änderungen sein oder auch Kommentare von Ihnen oder von Mitautoren. Wenn es irgend geht, sollten Word-Dokumente daher vor dem Versenden **in PDF umgewandelt** werden.

Soll der Empfänger das Dokument bearbeiten können, bietet sich ein **Abspeichern im RTF-Format** an. Dieses kann von allen gängigen Textverarbeitungen gelesen und geschrieben werden und besitzt keine eigene Makrofunktionalität. Um lediglich die Bearbeitung beim Empfänger zu gewährleisten, ist **RTF dem DOC-Format vorzuziehen** .

Ist das Word-Format unverzichtbar, achten Sie unbedingt darauf, die Datei vorher unter einem neuen Namen abzuspeichern (Menüeintrag "Datei / Speichern unter..."), um die Revisionsinformationen darin zu entfernen. **Versenden Sie anschließend nur diese neue Datei** !

Teil II: Der Empfang von eMails:

1. Der Betreff

- Ist der Betreff **sinnvoll** ?
- Ist der Betreff in der vom Absender **gewohnten Sprache** ?
- Hat der Betreff einen **Bezug** zu dienstlichen Themen und Aufgaben?

Warum?

Automatisch generierte Nachrichten von Mail-Würmern enthalten häufig allgemeine Betreffzeilen, die entweder inhaltsleer sind ("Hi!") oder die Aufmerksamkeit des Empfängers erwecken sollen ("Bilder von der letzten Party"). Da viele Mail-Würmer aus dem englischsprachigen Raum stammen, sind häufig die Betreffzeilen ebenfalls englisch. Daher sollte eine englische Betreffzeile von einem deutschen Absender zumindest zur Vorsicht animieren.

2. Der Mailtext

- Hat die Mail einen **Textteil** ?
- Werden Sie als Empfänger **persönlich angesprochen** ?
- Ist der Text in der vom Absender **gewohnten Sprache** ?
- Ist der Text im vom Absender **gewohnten Sprachstil** ?
- Wird ein beigefügter **Anhang im Text erwähnt** ?

Warum?

Auch hier geht es darum, automatisch erzeugte Mails zu enttarnen. Eine fehlende Anrede oder gar kein Mailtext deuten darauf hin.

Auch die Sprache der Mail ist wichtig. Schreibt ein deutscher Absender plötzlich englische Mails, ist Vorsicht geboten. Es könnte sein, dass er die Mail nicht selbst verfasst hat. Ebenso, wenn der Sprachstil sich signifikant unterscheidet: Eine Versicherung, in deren Mail "heiße Links zu zügellosen Webseiten" versprochen werden, ist entweder geschäftsuntüchtig oder von einem Mail-Wurm befallen.

Möglich ist dabei auch eine Adressfälschung. Wie die unter ULD-Absender verschickten Spam-Mails gezeigt haben, muss der eingetragene Absender nicht zwangsläufig auch der Urheber sein. Achten Sie deshalb auf Ungereimtheiten zwischen Absender und zugehöriger Mail.

Wer einen Anhang verschickt, sollte dies in der Mail kurz erwähnen und ggf. erklären, worum es sich dabei handelt. Es gilt nicht nur als schlechter Stil, unkommentierte Anhänge zu versenden, man kann so auch dem Empfänger einen kleinen Hinweis vermitteln, dass der Anhang echt und beabsichtigt ist.

3. Der Anhang

- Wird der Anhang vom Absender **erwartet** ? (Erwähnung im Mailtext, per Telefon oder auf anderem Wege)

- Handelt es sich um ein **Dokument oder ein Programm** ?

Warum?

Mails, die überraschende Anhänge enthalten, sind verdächtig. Niemand hängt eine Datei an eine Mail, ohne darüber ein Wort der Erklärung zu verlieren, stimmt's?

Wenn ein Anhang einer Mail beigefügt wurde, überprüfen Sie unbedingt, um welchen Typ von Datei es sich handelt, **bevor sie darauf klicken** ! Dokumente sind dabei, abhängig vom Typ, ungefährlich oder potentiell gefährlich. **Programme sind in 99,9% der Fälle gefährlich!**

Teil III: Informationen zu Dateitypen und Erweiterungen:

Der **Dateityp** ergibt sich aus der Endung, der sog. Extension. Bei aufsatz.doc handelt es sich also um ein Word-Dokument (Endung doc). Beachten Sie, dass **nur die letzte Extension** den Dateitypen bestimmt!

Aufsatz.**doc** : Word-Dokument

Aufsatz.doc.**exe** : Ausführbares Programm, **wahrscheinlich schädlich**.

Auch die Endung .com stellt ein ausführbares Programm dar. Bei einem **Dateianhang** namens **www.webseite.com** handelt es sich also nicht um einen Internetlink, sondern um eine ausführbare Datei!

Öffnen Sie diese nicht.

Das betrifft selbstverständlich nicht Internetadressen, die im Text einer eMail erwähnt werden. Wenn Sie diese anklicken, wird der Browser gestartet und die angegebene Webseite aufgerufen.

Eine Liste der gebräuchlichsten Dateitypen (ohne Anspruch auf Vollständigkeit) finden Sie im Internet unter http://www.datenschutzzentrum.de/selbstdatenschutz/internet/mail/dateitypen.htm **oder als gesondertes Dokument: „Virenmail Dateitypen.pdf“**

Diese und weitere Informationen finden Sie auch unter:
http://www.datenschutzzentrum.de/selbstdatenschutz/internet/mail/leitfaden.htm