linCK-IT GmbH & Co. KG

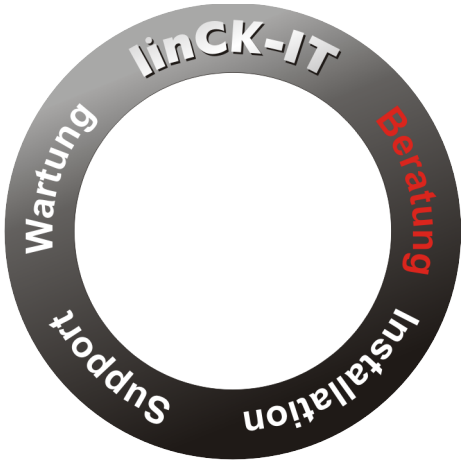
linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)

Netzwerklösungen
IT-Consulting
IT-Services
IT-Security

Katastrophenvorsorge
VoIP Telefonanlagen
Internetprojekte
Migrationen

Bei uns
ist Ihre IT
in guten Händen.

eMail – wie erkenne ich SPAM?



Ihr Ansprechpartner

Dipl.-Kfm.
Thomas Carlile
IT-Berater

Telefon: 089 5404748-10
tc@linck-it.de

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: (+49) 089 5404748-0
info@linck-it.de
http://linck-it.de
http://www.mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Das SPAM-Problem

Mails werden leider nicht nur für seriöse Kommunikation genutzt. Häufig landen Mails im Posteingang, die dem Anwender Artikel und Dienstleistungen andienen, Schadsoftware übermitteln oder den Anwender dazu verleiten wollen, Internetseiten zu besuchen, wo er seinen Rechner entweder mit Schadsoftware infiziert oder aber vertrauliche Daten eingeben soll („Phishing“). Die Varianten an Mails, die etwas mehr oder weniger Unseriöses von Ihnen fordern, sind zahlreich und werden gerne unter dem Begriff „SPAM“ (frei übersetzt „Abfall“ oder „Müll“) zusammengefasst.

Schadsoftware wird in Mails meist über Dateianlagen verbreitet oder über Links, die der Empfänger anklicken muss. In den HTML-Code der Mail eingebettete Schädlinge sind glücklicherweise nur selten zu beobachten. Macht sich eine Mail bereits durch Betreff und Absenderadresse verdächtig und wurde durch den SPAM-Filter bereits markiert, besteht keine Notwendigkeit sie zu öffnen – wir empfehlen in diesem Fall, sie nicht zu lesen.
Sind Absender und Betreff einer Mail aber unverdächtig oder lassen nur vermuten, dass es sich um SPAM handelt, muss die Mail geöffnet werden. Erst dann lassen sich weitere Erkenntnisse gewinnen (siehe Liste weiter unten). Wer etwas mehr Sicherheit beim Lesen solcher Mails haben möchte, sollte einen Blick auf unsere Tipps zur Einstellung der Leseansicht bei Mailprogrammen weiter unten werfen.

In der Regel bilden Virenscanner und Spamfilter einen sehr guten Schutz. Im Firmennetzwerk sind diese zentral verwaltet und an allen Rechnern verfügbar.

Aber natürlich ist keine Software fehlerfrei, so daß es vorkommen kann, daß eine Mail als SPAM klassifiziert wird, die Sie eigentlich gerne bekommen hätten („false positive“), oder eine SPAM-Mail nicht erkannt wird und ungekennzeichnet im Posteingang verbleibt. Auch Virenscanner scheitern gerne mal bei brandaktuellen Viren oder stufen eine Datei als Virus ein, die in Wahrheit völlig harmlos ist.

Gerade bei Mails fragen sich Anwender häufig: „Wie kann ich SPAM erkennen?“
Mit ein paar einfachen Prüfkriterien zeigen viele Nachrichten ihren wahren Charakter.

Wenn Sie (oder einer Ihrer Kolleginnen/Kollegen) eine Mail erhalten, auf die eines oder mehrere der folgenden Kriterien zutrifft, handelt es sich mit hoher Wahrscheinlichkeit um eine unerwünschte Werbemail (SPAM), den Versuch an vertrauliche Informationen zu gelangen, oder den Rechner des Mailempfängers mit Schadsoftware zu infizieren.

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: (+49) 089 5404748-0
info@linck-it.de
http://linck-it.de
http://www.mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Hier also die 11-Punkte-Liste zur Erkennung von SPAM-Mails

1. Der Absender ist unbekannt bzw. es wurde kürzlich keine Mail an diesen geschickt, im Betreff wird jedoch mit dem Kürzel „Re:“ oder „AW:“ oder ähnlichem suggeriert, daß auf eine Mail von Ihnen geantwortet wurde.
2. Die Mail ist in einer Sprache verfasst, in der Sie normalerweise nicht mit Ihren Geschäftskontakten kommunizieren.
3. Die Mail wurde gemäß Mailsignatur aus einem Land verschickt, in dem Sie keine Geschäftskontakte haben.
4. Die Sprachen von Absender-Land und Mailtext passen nicht zusammen.
5. Der Inhalt der Mail ergibt in Ihrem geschäftlichen Kontext keinen Sinn bzw. dient Dienste / Produkte an, an denen Sie definitiv nicht interessiert sind.
6. Es sind potenziell gefährliche Dateianhänge beigelegt mit der Endung .zip, .exe, .com, .bat, .scr, .js, .vbs, oder ähnlichem (Erkennung erfordert geeignete Einstellung im Mailprogramm, s.u.).
7. Ihr Spamfilter klassifiziert die eingehende Mail als SPAM.
8. Ihr Virenscanner schlägt an, weil ein potenziell gefährlicher Inhalt in der Mail gefunden wurde.
9. Die Mail sieht „echt“ aus, weist aber kleine Fehler auf (formelle oder textliche oder beides). Beispiele: Eine Telekom-Rechnung, die nicht Ihren Namen, Wohnort und das richtige Buchungskonto enthält, oder eine UPS Zustellbenachrichtigung ohne die korrekte Kontrollnummer, oder die Mail von einem Lieferanten ohne Nennung Ihrer Kundennummer.
10. Die Mail sieht „echt“ aus, aber der vermeintliche Absender verschickt normalerweise keine solchen Mails. Beispiele: die GEZ (aka „Beitragsservice von ARD, ZDF und Deutschlandradio“) schickt Ihnen eine Mail mit angehängter Rechnung. Das macht die GEZ nicht, muss also eine Fälschung sein. Oder Sie bekommen von Amazon eine Mahnung oder Rechnung, sollen dazu aber einen potenziell gefährlichen Anhang oder eine fremde Webseite öffnen - auch das dürfte sehr ungewöhnlich sein.
11. Links, die in der Mail angezeigt werden (bitte den Mauszeiger über dem Link schweben lassen ohne ihn anzuklicken – dann bekommen Sie meist den wahren Link angezeigt!), führen nicht dorthin, wo Sie es sich erwarten. Oder der Mailabsender hat eine ungewöhnliche Mailadresse. Beispiele: Eine Mail von Amazon fordert Sie auf, Ihr Passwort zu ändern, der Link zeigt aber nicht auf amazon.de oder amazon.com, sondern auf eine ähnliche Domain oder gar eine völlig andere Domain. Oder der Absender scheint „PayPal“ zu sein, die Mailadresse lautet aber „martin1982@ckcargo.co.uk“ oder „rechnung@paypal-services.co.ua“ (besonders gemein).

Es erfordert eigentlich nur wenig Übung, um anhand dieser Kriterien selbst entscheiden zu können, ob eine Mail SPAM und damit entweder nur unerwünscht oder sogar gefährlich ist, oder ob es sich um eine Geschäftsmail handelt.

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: (+49) 089 5404748-0
info@linck-it.de
http://linck-it.de
http://www.mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Da einige der oben genannten Punkte nur vom Mailempfänger selbst beurteilt werden können, ist eine Klassifizierung durch Dritte (dazu zählt auch Ihr Netzwerkadministrator) deutlich schwieriger, als wenn Sie diese Beurteilung selbst vornehmen. Im Zweifelsfall wenden Sie sich aber lieber an Ihren Administrator, bevor Sie verdächtige Mailanhänge öffnen und auf seltsame Links in der Mail klicken.
Oder lassen die Mail einfach dort, wo sie von Ihrem Spamfilter oder der Virenschutzlösung hin verbannt wurde: Im SPAM-Ordner oder in der Virenquarantäne.

5 Einstellungen für eine sicherere Mailansicht

Viele erwarten von Mails, daß sie ebenso ansprechend designed werden, wie Texte aus einer Textverarbeitung oder Hochglanzbroschüren. Das funktioniert mit reinen Textnachrichten nicht – außer man hängt den „hübschen“ Teil als PDF-Dokument an (was niemand macht). Die Lösung für dieses Problem wurde schnell gefunden: die HTML-Mail war geboren. Sie ermöglicht ein Layouten wie bei Internetseiten. Und Inhalte wie bei Internetseiten. Und damit auch Schadcode wie bei Internetseiten.
Ein paar einfache Einstellungen in Windows und Mailclient machen den Umgang mit Mails sicherer:

1. Im Windows Datei-Explorer die Option „Erweiterungen bei bekannten Dateitypen ausblenden“ deaktivieren. Damit werden nicht nur die Namen von Dateien angezeigt, sondern auch die kurze Erweiterung, die auf den Dateityp hinweist (z.B. .docx, .odf, .exe, .js, .vbs, .jpg, etc.). Wichtiger Effekt des Deaktivierens der Ausblende-Optionen: erhalten Sie per Mail eine ausführbare „.exe“-Datei, die als Bild getarnt ist (z.B. „.jpg“), wird der komplette Dateiname angezeigt, z.B.: harmlosaussehend.jpg.vbs. Bei aktivierter Ausblende-Option hätte die Datei so ausgesehen: harmlosaussehend.jpg. Die Dateiendung „.vbs“ wäre nicht offensichtlich geworden, beim Doppelklick auf das vermeintliche Bild hätten Sie wahrscheinlich ungewollt Schadsoftware installiert.
2. Will man vermeiden, sich einen in eine HTML-Mail eingebetteten (oder nachgeladenen) Schädling einzufangen, muss man in seinem Mailclient einstellen, daß Mails als reine Textnachrichten angezeigt werden. Das ist zwar nicht so hübsch wie das Erscheinungsbild oft aufwändig gestalteter HTML-Mails, erfüllt aber seinen Zweck. Und Schadcode muss leider draußen bleiben.
3. Als Alternative kann oft die Anzeige von „vereinfachtem HTML“ ausgewählt werden. Damit werden nicht alle HTML-Befehle umgesetzt und Sie sind besser geschützt als bei komplettem HTML.
4. Lassen Sie im Mailprogramm immer den vollständigen Namen eines Absenders anzeigen, inklusive Mailadresse. Beispiel: statt nur „TC“ wird dann angezeigt „Thomas Carlile <tc@linck-it.de>“. Oft verwenden Spammer einen vertrauenerweckenden Absendenamen wie „Amazon“ oder „DHL Rechnungsversand“, machen sich aber nicht die Mühe, auch die Mailadresse zu manipulieren. Sehen Sie dann einen Absender wie beispielsweise „DHL Onlinerechnung <ozfa@inowa.co.ua>“, sollten Sie sehr aufmerksam werden.
5. Im Mailprogramm das automatische Nachladen externer Inhalte abschalten. Diese können beim Anzeigen einer Mail, die vertrauenswürdig erscheint, auf Wunsch nachgeladen werden.
6. Deaktivieren der Option „Anhänge eingebunden anzeigen“. Damit haben Sie die Wahl, ob Sie den Anhang öffnen oder nicht.

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: (+49) 089 5404748-0
info@linck-it.de
http://linck-it.de
http://www.mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Einen hundertprozentigen Schutz gibt es natürlich nicht und Sicherheit ist immer auch etwas aufwändig. Aber wenn Sie Ihre kognitiven Fähigkeiten kombinieren mit einem gut trainierten SPAM-Filter und einem zuverlässigen Virenschutz, ist das Risiko „eMail“ eigentlich gar nicht mehr so hoch, wie Sie vielleicht dachten.

Zu diesem und anderen IT-Themen beraten wir Sie gerne.
Besuchen Sie uns doch einfach mal im Internet unter https://www.linck-it.de
und sehen Sie, was wir alles für Sie tun können.

Mit besten Grüßen,

Ihre linCK-IT GmbH & Co. KG

Lesbarkeit vs. Geschlechter-gerechte Sprache

Aus Gründen der besseren Lesbarkeit und der Erhaltung des Leseflusses wurde auf allen Seiten bei der Bezeichnung der Personen / Personengruppen jeweils die männliche Form verwendet. So schließen Begriffe wie zum Beispiel „Mitarbeiter“, „Anwender, „User“, „Kollege“, „Administrator“ usw. sowohl männliche als auch weibliche Personen ein. Von jeglicher Art und Form der Diskriminierung distanzieren wir uns hiermit ausdrücklich.

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: (+49) 089 5404748-0
info@linck-it.de
http://linck-it.de
http://www.mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny