# linCK-IT GmbH & Co. KG

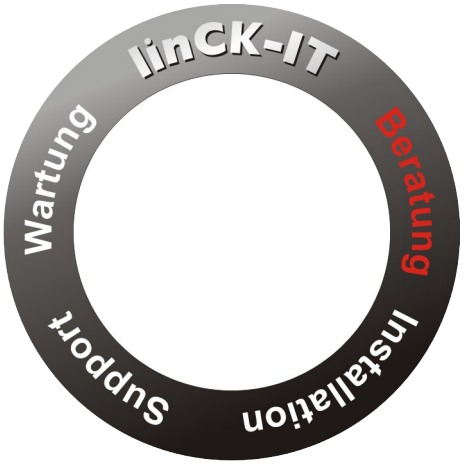
linCK-IT GmbH & Co. KG
Bretonischer Ring 10
85630 Grasbrunn (München)

Netzwerklösungen
IT-Consulting
IT-Services
IT-Security

Katastrophenvorsorge
VoIP Telefonanlagen
Internetprojekte
Migrationen

Bei uns
ist Ihre IT
in guten Händen.

# Schadsoftware im Posteingang




**Ihr Ansprechpartner**

Dipl.-Kfm.
Thomas Carlile
IT-Berater

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



linCK-IT GmbH & Co. KG
Bretonischer Ring 10
85630 Grasbrunn (München)
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 Malware – Problem

Schadsoftware (engl.: „Malware“) hat sich früher überwiegend über infizierte Datenträger verbreitet.

Heutzutage werden Viren, Würmer, Trojaner und Spyware überwiegend über dasjenige Medium verbreitet, das die meisten Nutzerzahlen aufweist: das Internet. Infizierte Webseiten befallen Rechner über Webbrowser, bösartige Mailanhänge bahnen sich den Weg zu nichtsahnenden Netzwerkinfrastrukturen.

Eines muss klar sein: einen hundertprozentigen Schutz gibt es bei keiner Sicherheitslösung – außer Sie nehmen Ihre Rechner vom Netz und spielen keine Software mehr ein. Virenscanner stellen zwar einen nicht zu vernachlässigenden Schutz dar, bieten aber keinen hundertprozentigen Schutz. Die Verbreiter neuer Schadsoftware haben immer einen kleinen Vorsprung, bis die Anbieter von Antivirenlösungen die neuen Schadcodes finden und Erkennungsmuster in ihren Virensignaturen implementieren können.

Man kann das Risiko aber deutlich senken: Durch den Einsatz von Virenschutzsoftware, das regelmäßige Einspielen von System- und Softwareupdates an Arbeitsplatzrechnern und Servern, den Entzug lokaler Adminrechte für normale Benutzer, das Setzen von Netzwerkrichtlinien. Einen wesentlichen Schutzfaktor stellt jedoch der Anwender selbst dar: er entscheidet, welche Webseiten er besucht, welche Mails er öffnet und welchen Mailanhängen er vertraut. Deshalb wollen wir im Folgenden ein paar Tipps für den verantwortungsvollen Umgang mit Mails geben, damit Sie es leichter haben, möglicherweise gefährliche Mails von wichtigen Geschäftsmails zu unterscheiden.

# Wie versuchen eMails, Schadsoftware auszuliefern?

Derartige Mails haben es zum Ziel, den Anwender dazu zu verleiten

- einen Link in der Mail anzuklicken, der auf eine Webseite führt, die Schadcode ins System einschleust. Hierbei wird über JavaScript versucht, eine Schwachstelle im Webbrowser und dem darunter liegenden Betriebssystem zu finden, um den Schadcode im System zu verankern. Von dort verbreitet er sich im ganzen (Firmen-)Netzwerk
- einen Dateianhang zu öffnen, der Schadcode ins System bringt und von dort wiederum auf das Netzwerk übergreift. Manchmal soll beim Öffnen der Mail eine Bestätigungsschaltfläche angeklickt werden, um einen angeblichen Versionskonflikt zu beheben (tun Sie das auf keinen Fall).

Zentrale Aufgabe des Anwenders beim Überprüfen des Posteingangs ist es damit, zu klassifizieren, welche Mails für ihn tatsächlich relevant und welche Mails unglaubwürdig sind. 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
Bretonischer Ring 10
85630 Grasbrunn (München)
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

# 11-Punkte-Liste zur Erkennung von Spam- / Viren-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, oder die Mail wurde gemäß Mailsignatur aus einem Land verschickt, in dem Sie keine Geschäftskontakte haben.
3. Die Sprachen von Absender-Land und Mailtext passen nicht zusammen.
4. Der Inhalt der Mail ergibt in Ihrem geschäftlichen Kontext keinen Sinn bzw. dient Dienste oder Produkte an, an denen Sie definitiv nicht interessiert sind.
5. Es sind ungewöhnliche und potenziell gefährliche Dateianhänge beigelegt mit der Endung .zip, .exe, .com, .bat, .scr, .js, .vbs, oder ähnlichem (Erkennung erfordert geeignete Einstellung im Mailprogramm, s.u.).
6. Ihr Spamfilter klassifiziert die eingehende Mail als SPAM.
7. Ihr Virenscanner schlägt an, weil ein potenziell gefährlicher Inhalt in der Mail gefunden wurde.
8. 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, eine UPS Zustellbenachrichtigung ohne die korrekte Kontrollnummer, oder die Mail von einem Lieferanten ohne Nennung Ihrer Kundennummer.
9. 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 (bisher) 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 ist sehr ungewöhnlich.
10. Web-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 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).
11. Sie bekommen eine echt aussehende Mail, die inhaltlich nicht zu Ihrem Aufgabenbereich passt. Beispiele: Sie sind Berater und bekommen ein Bewerbungsschreiben, eine Lieferantenrechnung, eine Rechnung der Telekom, eine UPS Zustellbenachrichtigung.



linCK-IT GmbH & Co. KG
Bretonischer Ring 10
85630 Grasbrunn (München)
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

# Relevanzbeurteilung

Scheitert die Einstufung gemäß obiger Liste, hilft oft eine einfache Relevanzbeurteilung:
Ist die Mail, unabhängig von ihrer anscheinenden Echtheit, überhaupt für Sie und Ihr Aufgabengebiet von Bedeutung? Wenn nein – warum sie dann öffnen? Ein paar Beispiele dazu:

- Wenn Sie nicht der Personalabteilung zuarbeiten, lassen Sie Bewerbungsmails ungeöffnet.
- Bestellen Sie keine Waren oder Dienstleistungen, dann ignorieren Sie Rechnungsmails.
- Haben Sie persönlich nicht etwas in den letzten Tagen per UPS, DHL, etc. verschickt, kümmern Sie sich nicht um Zustellbenachrichtigungen.
- Wenn Sie nicht vertrieblich tätig sind, lassen Sie ungewöhnlich formulierte Geschäftsanfragen ungeöffnet.

Macht sich eine Mail bereits durch unsere 11-Punkte-Liste oder die Relevanzbeurteilung verdächtig, besteht im Normalfall keine Notwendigkeit, sie zu öffnen – wir empfehlen in diesem Fall, sie nicht zu lesen. Wenn Ihr SPAM-Filter sie bereits markiert hat, ist ebenso Vorsicht geboten.

Es erfordert eigentlich nur wenig Übung, um anhand der genannten 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.

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 trotzdem 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 hinverbannt wurde: Im SPAM-Ordner oder in der Virenquarantäne.

# Ich bin unsicher – was jetzt?

Es wird immer wieder vorkommen, dass Sie eine Mail bekommen, bei der Sie nicht sicher sind, wie Sie mit ihr umgehen sollen. Ist der Link in der furchtbar interessanten Mail vielleicht doch harmlos?
Ist die im Word-Format beigelegte Bewerbung, die Sie als Personalsachbearbeiter ja eigentlich bearbeiten müssen, mit Schadsoftware verseucht? Ist die per Mail eingegangene Rechnung, die Sie für die Buchhaltung benötigen, echt? Hier hilft manchmal nur Ausprobieren. Aber das müssen Sie nicht unbedingt auf Ihrem eigenen Rechner tun, hierfür gibt es spezialisierte Dienstanbieter wie z.B. „Virustotal“.

Der Dienstanbieter schreibt zu seinem Dienst:
„VirusTotal ist ein kostenloser Dienst, der verdächtige Dateien und URLs analysiert und das schnelle Erkennen von Viren, Würmern, Trojanern und jeglicher Art von Schadsoftware ermöglicht.“

„Jegliche“ Art von Schadsoftware ist vielleicht etwas übertrieben, aber die Prüfung hochgeladener Dateien nach eigenen Angaben mit mehr als 70 Virenscannern ist extrem hilfreich.



linCK-IT GmbH & Co. KG
Bretonischer Ring 10
85630 Grasbrunn (München)
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

Detals zur Funktionsweise dieses Dienstes finden Sie unter
https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

Verdächtige Links und Dateien lassen Sie auf folgender Seite prüfen:
https://www.virustotal.com/de/
Dazu müssen Sie den Dateianhang nur auf Ihrem Rechner speichern (NICHT öffnen!) und über das Webformular von Virustotal hochladen. Auf der Startseite des Dienstes finden Sie auch Angaben zu Nutzungsbedingungen und Datenschutz.

Geben bei einer Prüfung durch Virustotal mehrere Virensuchengines den Befall durch Schadsoftware an, sollten Sie die Datei auf keinen Fall öffnen bzw. den geprüften Link nicht im Webbrowser aufrufen.

## Die neue Masche – Social Engineering

Bis hier war sicherlich einiges schon bekannt. Betrüger haben aber mittlerweile noch andere Tricks im Angebot, um Firmen und Privatleute um ihr Geld zu bringen. Man sucht sich in einer Firma eine Person heraus, die zunächst gezielt mit vertrauenswürdig erscheinenden aber verseuchten Mails angegriffen wird. Ist eine dieser Mailattacken erfolgreich, wird ein Schädling auf dem Rechner der betreffenden Person installiert (und evtl. auch im Netzwerk), der Informationen sammelt. Mit diesen Informationen wird es den Angreifern möglich, eine Mail an die ausgewählte Person zu schreiben, die wirklich vertrauenswürdig wirkt (Absender, Name und Mailsignatur sind OK). Sie soll sie dann dazu verleiten, eine Zahlung zugunsten der Angreifer auszuführen.

Beispiele:

- Eine Buchhalterin oder Chefsekretärin bekommt von einem der Geschäftsführer die Anweisung, ihm für ein dringendes Geschäft oder zur Vermeidung von Strafe einen Geldbetrag auf ein bislang unbekanntes (Auslands-) Konto zu überweisen. Natürlich soll sie Stillschweigen bewahren.
- Ein Geschäftsführer bekommt von seinem Mitgeschäftsführer, der sich gerade im Urlaub befindet, die Nachricht, er sei bestohlen worden und benötige jetzt dringend eine größere Summe Geld, die auf ein ihm bisher unbekanntes Konto oder einen Barauszahlungsdienst, wie z.B. „Western Union“, überwiesen werden soll.
- Ein Angestellter schickt eine Mail an die Personalabteilung mit der Bitte, das Konto für seine Gehaltszahlung zu ändern.
- Ein entfernter Verwandter / Bekannter meldet sich mit einer finanziellen Notlage. Das ist eine ähnliche Masche, wie Anrufe von vermeintlichen Enkeln bei ihren Großeltern, nur dass die Masche per Mail durchgezogen wird und nicht speziell auf ältere Menschen abzielt.
- Ein angeblicher Student bittet um eine Fachexpertise, damit er seine Facharbeit (o.ä.) darauf aufbauen kann. Dazu muss der Mailempfänger natürlich ein (verseuchtes) Office-Dokument öffnen.



linCK-IT GmbH & Co. KG
Bretonischer Ring 10
85630 Grasbrunn (München)
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

**Was können Sie hier im Zweifelsfall tun?**

- Versuchen Sie, den vorgeblichen Absender der Mail per Telefon zu erreichen. Aber verwenden Sie keine der Telefonnummern, die evtl. in der Mail aufgeführt sind, sondern rufen Sie ihn auf den Ihnen bekannten Nummern an. Besser den Chef oder den Ehepartner beim Abendessen gestört oder im Meeting, als unkontrolliert eine halbe Million nach Nigeria überwiesen zu haben.
- Als Angestellter lassen Sie sich am besten das „OK“ eines zweiten Geschäftsführers geben, falls der Vorgesetzte, der die Mail angeblich verfasst hat, nicht erreichbar ist.

# Schlusswort

Einen hundertprozentigen Schutz gibt es natürlich nicht und Sicherheit ist immer auch etwas aufwendig. Aber wenn Sie Ihre kognitiven Fähigkeiten kombinieren mit einem gut trainierten SPAM-Filter und einem zuverlässigen Virenschutz, ist das Risiko „eMail“ 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
Bretonischer Ring 10
85630 Grasbrunn (München)
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

# Anhang: 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 aus Bequemlichkeit fast niemand macht). Die Lösung für das 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
Bretonischer Ring 10
85630 Grasbrunn (München)
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