

linCK-IT GmbH & Co. KG

linCK-IT GmbH & Co. KG
Südliche Münchner Straße 46a
D-82031 Grünwald

Netzwerklösungen
Security-Lösungen
IT-Consulting
IT-Services

Katastrophenvorsorge
Internetprojekte
Migrationen
Schulungen

Bei uns
ist Ihre IT
in guten Händen.

Viren, Virus-Warnmeldungen und IT Security

Virenwarnungen

Bei einigen Virenwarnungen handelt es sich um sog. "Hoaxes".

Ein Hoax stellt selbst eine Art Virus dar (ist aber keines!) - es dient einzig dem Ziel, Mailserver durch eine Flut von Warnmeldungen zu belasten, oder User dazu zu verleiten, Systemdateien selbst zu löschen.

Beispiel:

Die immer wieder gerne gelesenen Warnungen vor dem Bildschirmschoner "Budweiser Frösche", vor Mails mit Nacktbildern von Stars wie Anna Kournikova, der angeblich infizierten Systemdatei jdbgmgr.exe u.v.a.; vgl. hierzu Infoseiten von Symantec, CA oder NAI, z.B. unter dem Link: <http://securityresponse.symantec.com/avcenter/venc/data/pf/jdbgmgr.exe.file.hoax.html>

Wirklich gefährliche Viren zeichnen sich neben der i.d.R. unmittelbaren Schadenswirkung (es wäre ja unintelligent vom Virus-Programmierer auf ein Gegenmittel von Symantec, CA, NAI etc. zu warten) durch die hohe Verbreitungsgeschwindigkeit aus - ohne Zutun des Users. nach der Verbreitung über das firmeneigene Mailsystem an alle Kontakte entfaltet sich das Schadenspotential meist umgehend.

Mittlerweile sollte jedes Unternehmen über aktuelle und sich selbsttätig aktualisierende Virens Scanner an Servern und Arbeitsplätzen als Bestandteil einer firmenweiten Security-Lösung verfügen. Und diesem Virens Scanner sollte man dann auch ein klein wenig vertrauen schenken.

Sollten Sie per eMail eine Nachricht bekommen mit dem Hinweise, von Ihnen wäre eine virenverseuchte eMail verschickt worden: dies ist nicht unbedingt ernstzunehmen – vor allem wenn der Absender nicht bei Ihren Kontakten gelistet ist.

Mail-Viren fälschen oftmals Absenderadressen, so daß die automatische Antwort der serverbasierten Mailvirens Scanner an den vermeintlichen Absender einer virenbehafteten eMail ("Sie haben eine virenverseuchte Mail verschickt..." o.ä.) leider nicht immer den Tatsachen entspricht.

Von einer sofortigen Weiterleitung von Viruswarnmeldungen, die ja durchaus auch Hoaxes sein können, raten wir ab, da dies Ihre Geschäftspartner unnötig verunsichert.

Bitte prüfen Sie vorab Viruswarnungen auf deren Wahrheitsgehalt, oder befragen Sie hierzu Ihren Netzwerkbetreuer oder IT-Dienstleister.

Ein kurzer Blick auf die Infoseiten renommierter Antivirus-Lösungsanbieter, wie z.B. CA (Computer Associates), Symantec, NAI (McAfee) oder TrendMicro schafft hier meist schnell Klarheit.

linCK-IT GmbH & Co. KG

linCK-IT GmbH & Co. KG
Südliche Münchner Straße 46a
D-82031 Grünwald

Netzwerklösungen
Security-Lösungen
IT-Consulting
IT-Services

Katastrophenvorsorge
Internetprojekte
Migrationen
Schulungen

Bei uns
ist Ihre IT
in guten Händen.

Viren, Virus-Warmmeldungen und IT Security

Schutz vor Viren

Es gibt einige Sicherheitsvorkehrungen, die das Risiko einer Virusinfektion minimieren. Diese im Folgenden gelisteten Punkte empfehlen wir jedem Unternehmen als Standard:

- *Einsatz einer mehrstufigen netzwerkweiten Virenschutzlösung:*
 - I.: Virens Scanner dienen als primärer Virenschutz für Clients, Server und Groupware-Lösungen – natürlich zentral administrierbar.
 - II.: Zusätzlich ist der Einsatz eines Mailproxies empfehlenswert. Dieser prüft eingehende Mails nach den Kriterien Dateianlagen (gesperrt oder freigegeben?), Spam und Schlüsselwörter. Je nach Scanergebnis kann eine eingehende Mail geblockt oder durchgelassen werden.
- *Versand von Mails im Nur-Text-Format (kein HTML oder MS-RTF).*

Grund: HTML-Mails können aktive Elemente enthalten, bei denen eine Virenverseuchung möglich ist. Textnachrichten enthalten nur Text. Der Verlust der Formatierungsoptionen ist meines Erachtens zu verschmerzen.

Geschäftspartner sollten dahingehend beeinflusst werden, daß Mails an Ihre Mailadressen ebenfalls nur als Textnachrichten verschickt werden (i.d.R. konfigurierbar im Mailclient).
- *kein unaufgeforderter Versand ausführbarer Dateien (.exe, .com, .bat, etc.)*

Ausführbare Dateien können a) Viren enthalten und b) von Virens Scannern automatisch geblockt werden.
- *Konfiguration der Vollanzeige von Details im Explorer (um Dateiendungen anzuzeigen).*

Nur so kann bei einer Anlage erkannt werden, ob die Dateiendung .jpg (Bild) oder .jpg.vbs (VB-Script) gefährlich ist.
- *Vorsicht beim Öffnen von Mails, die in einer Fremdsprache abgefaßt sind.* Wenn Sie von einem Geschäftspartner z.B. nicht eine englische eMail erwarten, sollten Sie englische Mails mit ungewöhnlichem englischen Betreff ungefragt löschen und rückfragen. Grund: in derartigen Mails sind oft Viren versteckt (in der Anlage oder der HTML-Mail selbst).
- *Ausschalten der Schnellansicht für eMails (i.d.R. konfigurierbar im Mailclient).*

Grund: die Schnellansicht öffnet für diese Schnellansicht UNGEFRAGT die Mail und aktiviert damit (bei HTML-Mails) ein potentielles Virus. Dies sollte unbedingt verhindert werden.
- *Anzeige eingehender Mails als reine Textnachricht:*

aktive Inhalte in HTML-Mails können so umgangen werden.
- *Versand von Dokumenten in einem „harmlosen“ Textformat wie RTF.*

Grund: Office-Dokumente können virulente VisualBasic-Scripte enthalten. Sollen Texte editierbar versandt werden, so bietet sich das universelle und allen Systemplattformen zugängliche RTF (Rich Text Format) an, in dem umfangreiche Textformatierungen erhalten bleiben. Nicht editierbare Texte können als pdf-Datei übermittelt werden, solange in diesen Dateityp keine aktiven Komponenten vom Hersteller Adobe integriert werden (derzeit wurden bereits erste pdf-Viren gemeldet).

linCK-IT GmbH & Co. KG

linCK-IT GmbH & Co. KG
Südliche Münchner Straße 46a
D-82031 Grünwald

Netzwerklösungen
Security-Lösungen
IT-Consulting
IT-Services

Katastrophenvorsorge
Internetprojekte
Migrationen
Schulungen

Bei uns
ist Ihre IT
in guten Händen.

...

Es tauchen seit einiger Zeit zahlreiche eMails mit gefälschten Absenderkennungen (Headers) auf.

In diesen wird beispielsweise von einem Administrator-Account des hauseigenen Netzwerkes aus der Mailempfänger z.B. davon in Kenntnis gesetzt, daß sein Mailaccount wg. Mißbrauchs gesperrt wird. Zur Freischaltung des Mailaccounts soll eine Dateianlage geöffnet werden (z.B. ein pdf-Dokument), welche dann das Virus enthält.

Diese und andere Mails, die den Start einer unbekanntem Dateianlage fordern, sollten vor dem Start der Dateianlage hinterfragt werden. Viele dieser Mails können schon deshalb als unecht identifiziert werden, weil deren Inhalte nicht mit den Gepflogenheiten der hauseigenen IT konform gehen.

Sollten Sie oder einer Ihrer Geschäftspartner im Bereich Virenschutz, Spamfilter oder allgemein IT-Security noch Informationsbedarf haben, so stehen wir, die **linCK-IT GmbH & Co. KG**, gerne als Berater und Dienstleister zur Verfügung, um mit Ihnen gemeinsam eine unternehmensweite Security-Lösung zu konzipieren / implementieren, die Ihren individuellen Anforderungen gerecht wird:

linCK-IT GmbH & Co. KG

...Ihr IT-Partner für den Mittelstand

Tel. 0 89 / 69 37 91-70
eMail info@linck-it.de
www <http://linck-it.de>



linCK-IT GmbH & Co. KG

– Security-Lösungen für den Mittelstand –

Internet-Firewall

Sichern Sie Ihr Netzwerk gegen Angriffe aus dem Internet ab:
damit *Ihre* Daten auch wirklich *Ihre* Daten bleiben.

Wir unterstützen Sie dabei.
Mit Lösungen für kleine und mittelständische Unternehmen, die nicht nur *zuverlässig* sondern auch *bezahlbar* sind.

Spam-Filter

...halten Ihr eMail-Postfach frei für wirklich *wichtige* Nachrichten.

„Zeit ist Geld“ sagt ein altes Sprichwort.

Lassen Sie sich nicht Ihre wertvolle Zeit stehlen.



Virenschutz

Schützen Sie Ihre Daten vor Viren.

Eine netzwerkweite Antivirus-Lösung verhindert Datenverlust und damit Ausfallzeiten.

Virenschutz für Arbeitsplatzrechner und Server muß nicht teuer sein.

Datenverlust ist oft unbezahlbar.



Ihr IT-Partner

Wir helfen Ihnen bei der Bewältigung der Herausforderungen in Ihrem Netzwerk:

schnell, professionell und diskret.

Rufen Sie uns an und vereinbaren Sie noch heute einen Beratungstermin mit uns — damit Sie schon morgen den Kopf frei haben für Ihr *eigentliches* Business.

Bei uns ist Ihr Netzwerk in guten Händen.

www.linck-it.de