IT-Sicherheit für Selbständige und Kleinunternehmer

» Souverän entscheiden » Einfach schützen » Unternehmenserfolg absichern

2 Schulungsunterlagen für Ihre Mitarbeiter

Mithilfe dieser Checkliste helfen Sie Ihren Mitarbeitern, betrügerische E-Mails sofort zu erkennen und zu beseitigen.

3 Leserfragen individuell vom Experten gelöst

IT-Experte Manfred Kratzl gibt Lösungen für unsichere WLAN-Netzwerke oder veraltete Software auf Firmencomputern.

4 Sichern Sie sich gegen Datenverlust ab

Datenverlust kann existenzbedrohend sein. Mit diesen Sicherungsstrategien beugen Sie allen Ursachen dafür vor.

7 Gehen Sie souverän mit Virenbefall um

Säubern Sie in 6 einfachen Schritten Ihre infizierten Rechner und schließen Sie die Sicherheitslücken selbständig.

„Riskieren Sie nicht Ihre unternehmerische Existenz“

Gehören auch Sie zu den Unternehmen, die nicht wissen, ob sie alle kritischen Sicherheitslücken geschlossen haben? Ob Ihre Datensicherung vollständig ist, wenn Sie sie im Ernstfall benötigen?

Konzentrieren Sie sich endlich wieder auf Ihr Kerngeschäft: Schützen Sie ab sofort Ihr Unternehmen vor Datenspionage und Schadprogrammen aus dem Internet und schließen Sie alle IT-Sicherheitslücken im Handumdrehen. Treffen Sie lästige IT-Sicherheitsentscheidungen sicher und effizient und sparen Sie Zeit bei der Durchführung notwendiger Schutzmaßnahmen durch übersichtliche Checklisten und Mitarbeiterschulungsunterlagen.

Die geprüften und direkt umsetzbaren Anleitungen, die ich Ihnen in **IT-Sicherheit für Selbständige und Kleinunternehmer** gebe, helfen Ihnen dabei! Sie sind konkret auf Ihre Unternehmersituation zugeschnitten.

Mit freundlichen Grüßen,

Ihr

Manfred Kratzl,
IT-Sicherheitsexperte
und Chefredakteur

PS: Sparen Sie die Kosten für teure IT-Abteilungen und IT-Berater: Fragen Sie immer zuerst mich, wenn es um die Sicherheit Ihrer Daten und Computer geht. Sie erreichen mich ganz einfach und kostenlos per E-Mail: redaktion@sichere-it-deutschland.de.

E-Mail-Bedrohungen ausschalten

Schützen Sie Ihr Unternehmen vor den 3 gefährlichsten Betrugsfällen

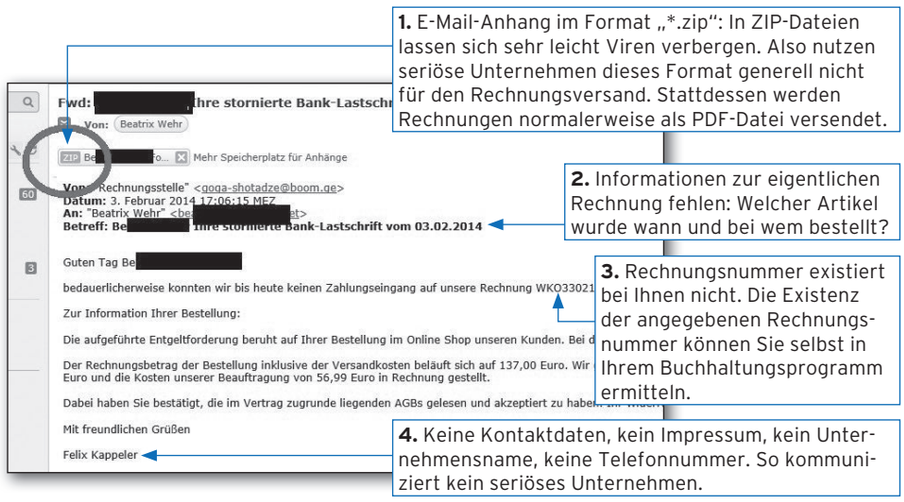
Online-Kriminelle und leider auch manche Ihrer Wettbewerber versuchen, per E-Mail das Vertrauen Ihrer Mitarbeiter zu gewinnen und sie zu unvorsichtigem Handeln zu verführen. Dabei werden immer raffiniertere Tricks angewendet. Ich zeige Ihnen, wie Sie Ihre Firma vor solchen Fallen schützen und Ihre Mitarbeiter schnell und effektiv schulen.

Sie und Ihre Mitarbeiter sind täglich mit vielfältigen und wechselnden Bedrohungen konfrontiert. Erklären Sie Ihren Mitarbeitern die folgenden drei Betrugsfällen, das jeweilige Gefahrenpotenzial und wie sie sich schützen können.

Betrugsfalle Nr. 1: Die unbezahlte Rechnung

Hacker versuchen, mit einer fingierten Zahlungsaufforderung einen Trojaner in Ihrem Netzwerk zu platzieren. Sie erhalten eine E-Mail mit dem Hinweis auf eine scheinbar noch nicht bezahlte Rechnung. Dies erfordert eigentlich ein sofortiges Handeln. Sie sollen verführt werden, den Rechnungsanhang zu öffnen.

Daran erkennen Sie den Betrugsversuch:



Diese gefälschte Rechnung verrät sich vor allem durch fehlende Angaben zum Einkauf und zum Einkäufer.

››› *Fortsetzung von Seite 1*

Betrugsfalle Nr. 2: Angebliche Probleme beim Telefon-Banking

Immer mehr Unternehmer führen ihre Bankgeschäfte online oder per Telefon durch – ein weiteres Feld für Betrugsversuche. Im folgenden Betrugsversuch besteht angeblich ein Problem mit Ihrer PIN und Sie werden in einer E-Mail aufgefordert, auf einen Link zu klicken, um Ihre PIN zu ändern.

Daran erkennen Sie den Betrugsversuch:

1. Ihre Bank wird Sie niemals auffordern, Ihre vertraulichen Daten im Internet oder telefonisch herauszugeben oder zu ändern.
2. Die persönliche Anrede fehlt in der Mail.
3. Aufbau einer Drohkulisse: Die „Bank“ droht mit Geldstrafe.


Postbank

www.postbank.de

Girokonto
Sparkonto
Kreditkarte

Online-Banking weltweit per Internet

Online-Zugriff auf Ihre Giro-, Spar- und Kreditkartenkonten

Mehrfach getestete und ausgezeichnete Sicherheitsstandards

Guten Tag,

Unser System hat festgestellt, dass Ihr Telefon-Banking PIN aus Sicherheitsgründen geändert werden muss. Bitte benutzen Sie dieses Formular um die Änderung Ihres Telefon-Banking PIN kostenfrei zu ändern.

Andernfalls müssen wir **Ihr Konto mit 14,99€ belasten** und die Änderung schriftlich über den Postweg bei Ihnen einfordern.

Ihren Telefon-Banking PIN können Sie hier oder wie folgt ändern:

1. Öffnen Sie die Datei in Ihrem Emailanhang und wählen Sie "öffnen mit" aus!
2. Füllen Sie alle Daten aus und klicken Sie dann auf "Daten absenden"!
3. Ihr Telefon-Banking PIN aktiviert sich nach 5-7Werktagen!

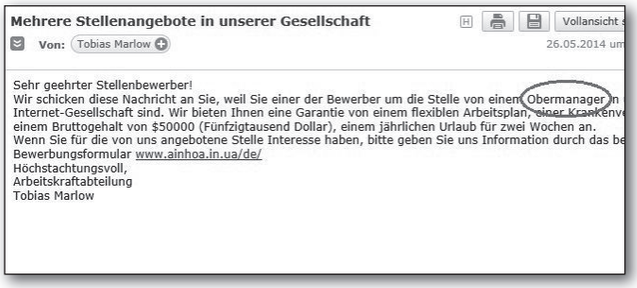
Für weitere Fragen steht unser Online Support unter direkt@postbank.de 24Std. für Sie zur Verfügung.

Gefälschte Postbank-Mail: Hier sollen Sie auf einen Link klicken, um sicherheitsrelevante Daten zu ändern.

Betrugsfalle Nr. 3: Das lukrative Jobangebot

Sie haben sich zwar nirgendwo beworben, aber das vermeintlich interessante Jobangebot kann man sich ja trotzdem mal ansehen? Auf diese Denkweise setzen Cyberkriminelle mit dem Trick der Jobangebote.

Daran erkennen Sie den Betrugsversuch:


Mehrere Stellenangebote in unserer Gesellschaft

Vollansicht

Von: Tobias Marlow

26.05.2014 um

Sehr geehrter Stellenbewerber!
Wir schicken diese Nachricht an Sie, weil Sie einer der Bewerber um die Stelle von einem Obermanager in Internet-Gesellschaft sind. Wir bieten Ihnen eine Garantie von einem flexiblen Arbeitsplan, einer Krankenv einem Bruttogehalt von $50000 (Fünfzigtausend Dollar), einem jährlichen Urlaub für zwei Wochen an.
Wenn Sie für die von uns angebotene Stelle Interesse haben, bitte geben Sie uns Information durch das be Bewerbungsformular www.ainhoa.in.ua/de/
Höchstachtungsvoll,
Arbeitskraftabteilung
Tobias Marlow

Betrugsversuch in Form eines dubiosen Stellenangebots: Die Mail ist schon deshalb verdächtig, weil sie unaufgefordert bei Ihnen eintrifft.

1. Die persönliche Anrede fehlt auch in dieser Mail.
2. Die Mail ist in holprigem Deutsch verfasst.
3. Der Link, den Sie anklicken sollen, weist durch seine Endung „ua“ auf eine Top Level Domain der Ukraine. Sehr viele Viren- und Hacker-Angriffe der letzten Jahre waren ukrainischer Herkunft. Bei Absendern mit dieser Top Level Domain sollten Sie also grundsätzlich sehr vorsichtig sein!

Das passiert, wenn Sie solche Links anklicken oder Dateien öffnen

Nach einem Klick auf die Links oder Anhänge werden Sie meist auf eine gefälschte Webseite geleitet, die der eigentlich erwarteten originalen Seite zum Verwechseln ähnlich sieht. Geben Sie hier Ihre Daten wie beispielsweise Passwörter ein, können Hacker diese auslesen. Beim Besuch der Webseite können Online-Kriminelle zusätzlich Schad-Software auf Ihren Computer laden.

Trojaner-Programme leiten dann Ihre vertraulichen Geschäftsdaten an den Server des Betrügers. Diese Daten enthalten zum Teil komplette Datensätze, beispielsweise Ihre geschäftliche Korrespondenz. Möglicherweise wird auch ein „Sperr-Trojaner“ installiert. Dieser sperrt den Zugang zu Ihrem PC und fordert ein Lösegeld für die Freischaltung.

Schulungsunterlage für Ihre Mitarbeiter

Checkliste: Daran erkennen Sie betrügerische E-Mails sofort

- ☐ Sie werden in der E-Mail nicht persönlich mit Ihrem Vor- und/oder Nachnamen angesprochen.
- ☐ Es werden Ihnen außergewöhnliche Dinge versprochen, wie Lotteriegewinne, angebliche Geheimnisse oder besonders lukrative Jobangebote.
- ☐ Die E-Mail ist in eher holprigem Deutsch verfasst.
- ☐ Sie werden zur Herausgabe persönlicher Informationen wie etwa einer PIN, eines Passworts oder Ihrer Konto- und Kreditkartendaten gedrängt.
- ☐ Eine Drohkulisse wird aufgebaut: Der Absender setzt Fristen, bis zu denen Sie etwas Bestimmtes tun müssen. Bei Nichterfüllen dieser Dinge droht er Ihnen mit Gebühren oder anderen Repressalien wie Kontensperrung.
- ☐ Die E-Mail enthält Datei-Anhänge im Format „*.exe“, „.scr“, „.vbs“ oder „*.rar“ und Sie werden gleichzeitig im Text der E-Mail dazu gedrängt, diese Anhänge anzuklicken bzw. zu öffnen.

Auswertung: Trifft nur einer dieser Checkpunkte auf Ihre E-Mail zu, sollten Sie vorsichtig sein. Klicken Sie keinesfalls die darin enthaltenen Links oder Anhänge an. Löschen Sie diese E-Mail bitte sofort – besonders wenn Ihnen der Absender unbekannt ist.