

Nachrichten Beitrag

Von: Elias Prohazka, Jonas Wiener, Jack Tahrioui, David Moors

1. Sensibilisieren für Risiken
 1. Spam
 1. E-Mail Anhänge
 2. Links
 2. Schadsoftware / Ad-Ware aus dem Internet
 1. Kann den PC für ein Botnetz missbrauchen
 2. Kann eingegeben Daten abfangen
2. Maßnahmen zur Vorbeugung
 1. Spam
 1. Nicht darauf antworten
 2. Auf Absender / Betreff überprüfen
 3. Keine Inhalte wie Links oder Anhänge anklicken
 4. Mehrere E-Mail Adressen verwenden (privat und geschäftlich)
 2. Schadsoftware
 1. Antiviren-Programm aktuell halten
 2. Nur verifizierte Software herunterladen (ggf. Software intern prüfen lassen)
3. Quelle für Hilfe
 1. Interne IT-Services
 2. Support des Herstellers der verwendeten Software

Sensibilisieren für Risiken

E-Mails können von verschiedenen unseriösen Absender stammen. Diese haben dabei keine guten Absichten und versuchen Daten von Ihnen zu erschwindeln. Achten Sie verstärkt auf die E-Mail Adresse des Absenders und auf den Betreff. Kommt ihnen dabei etwas nicht bekannt vor oder Sie kennen den Absender nicht, können Sie diese E-Mail beruhigt löschen oder zum Mindest nicht darauf antworten. Sollten Sie sich nicht sicher sein, öffnen Sie keine Anhänge oder Links aus dieser Mail.

Sollten Sie Software oder Tools aus dem Internet herunterladen und installieren wollen, achten Sie darauf ob diese tatsächlich von einer zertifizierten Hersteller Seite kommen. Fragen Sie ggf. Die IT-Abteilung Ihres Unternehmens um sicher zu gehen.

Hilfe können Sie immer bei den Herstellern einer Software oder der IT-Abteilung Ihres Unternehmens erhalten.