



E-Mails mit Dateianhängen

- Laut einer Berechnung des Deutschen Instituts für Wirtschaftsforschung aus dem Jahr 2015 entsteht durch **Schadsoftware**, die ebenfalls oft über E-Mails eingeschleust wird, ein Schaden von jährlich **knapp 1,2 Milliarden Euro** in Deutschland – nur bei Privatpersonen!
(Quelle: Deutsches Institut für Wirtschaftsforschung e.V. – DIW Berlin, https://www.diw.de/documents/publikationen/73/diw_01.c.498298.de/15-12-6.pdf, S. 301)
- Eine Online-Umfrage des Bundesamtes für Sicherheit in der Informationstechnik ergab, dass **jede dritte deutsche Firma** bereits teils erhebliche Ausfälle der IT-Infrastruktur durch Schadprogramme hatte. Und bei **drei Vierteln dieser Unternehmen waren E-Mail-Anhänge die Ursache**.
(Quelle: c't 2016, Heft 11, S. 29)

1. Überprüfe die E-Mail mit der bekannten Vorgehensweise auf Authentizität. Notiere die Ergebnisse.

Rechnung noch offen 25.03.2015 Nummer 80855672



Vollansicht



Von: Stellvertretender Sachbearbeiter Ebay AG

26.03.2015 um 04:17 Uhr



ZIP Rechnung an ...

"Stellvertretender Sachbearbeiter Ebay AG" <juergen.pentrup@online.de>

Guten Tag

Hier war die korrekte Anrede mit Vorname und Name eingetragen

das von Ihnen vorliegende Bankkonto wurde im Moment der Abbuchung nicht ausreichend gedeckt um die Lastschrift auszuführen. Sie haben eine nicht gedeckte Rechnung bei unseren Mandanten Ebay AG.

Aufgrund des bestehenden Zahlungsverzug sind Sie **gezwungen dabei** die durch unsere Tätigkeit entstandenen Kosten von 37,16 Euro zu bezahlen. Wir erwarten die Überweisung bis spätestens 30.03.2015 auf unser Konto.

Es erfolgt keine weitere Erinnerung oder Mahnung. Nach Ablauf der Frist wird die Angelegenheit dem Staatsanwalt und der Schufa übergeben. Eine vollständige Kostenaufstellung, der Sie alle Positionen entnehmen können, fügen wir bei. Für Fragen oder Anregungen erwarten wir eine Kontaktaufnahme innerhalb des gleichen Zeitraums.

Namens unseren Mandanten fordern wir Sie auf, die noch offene Gesamtforderung sofort zu bezahlen.

Mit freundlichen Grüßen

Stellvertretender Sachbearbeiter Zimmermann John

- Die Echtheit der Absenderadresse ist zwar unwahrscheinlich, aber nicht ganz auszuschließen, wenn ein externer Rechtsanwalt eingeschaltet wird.
- Grammatik und Rechtschreibung:
Zwei Formulierungen sind fehlerhaft.
- Die persönliche Anrede ist korrekt.
- Eine Internetrecherche nach „rechnung noch offen stellvertretender sachbearbeiter ebay“ führt zu dem Ergebnis:
„SPAM vom Sachbearbeiter Ebay AG, mal wieder wird versucht im Namen von Ebay an Daten zu kommen. ACHTUNG öffnen Sie auf keinen Fall den Anhang. Denn in diesen Zip-Dateien sind die „Viren“ versteckt.“ (Quelle: <https://verbraucherschutz.de/spam-vom-sachbearbeiter-ebay-ag/>)

- Beachte den **Dateianhang** („Rechnung an ...“.ZIP) – **nicht öffnen bzw. anklicken!**



Schadsoftware

2. Formuliere Unterschiede zwischen Viren, Würmern und Trojanern.

Viren werden aktiv, wenn eine infizierte Datei geöffnet wird und schreiben ihren Programmcode dann in weitere Dateien.

Würmer sind für die Fortpflanzung nicht unbedingt auf das Öffnen einer Datei angewiesen. Sie können sich auch selbsttätig in fremden Systemen einnisten und nutzen das System infizierter Computer, z. B. um die E-Mail-Adressen auszulesen und sich an alle Adressen zu senden.

Trojaner täuschen eine sinnvolle Anwendung vor, um den Nutzer dazu zu verleiten, die Datei mit dem Trojaner zu öffnen. Sie enthalten dann aber zusätzliche Funktionen, mit denen sie Schaden verursachen.

3. Nenne Beispiele für Schadfunktionen.

z. B.: Dateien verändern oder löschen.

Netzwerke durch hohen Datenverkehr blockieren.

Diebstahl von Zugangsdaten zum Online-Banking.

Einem Hacker die Möglichkeit eröffnen, beliebig auf den eigenen Rechner zugreifen zu können.

4. Du hast die E-Mail rechts erhalten. Statt „Mein Freund“ war der Name eines deiner Freunde bei WhatsApp eingetragen.

- Beschreibe, wie du mit der E-Mail umgehst. Begründe dein Vorgehen.

Hinweis: Sprachnachrichten in WhatsApp werden im Opus-Format versendet.

Allgemein werden Audiosignale auch oft im MP3-Format gespeichert.

In beiden Formaten liegen die Daten hoch komprimiert vor, so dass es weder notwendig noch sinnvoll ist, solche Dateien noch zu zippen.

Es sind auch schon Betrugsversuche mit WAV-Dateien aufgetaucht. Dabei handelt es sich zwar um ein Audioformat, das aber nicht heruntergeladen und extrahiert werden muss, wie es in dem Text der betreffenden E-Mails beschrieben ist. Vielmehr liegt hier eine versteckte ZIP-Datei vor.

Maßnahme: Sofort löschen bzw. unter Spam einsortieren!

Begründung: WhatsApp in der Absenderadresse ist falsch geschrieben.

Der Dateianhang im ZIP-Format ist nicht plausibel.

- Was wird sich wohl in dem Dateianhang befinden? Begründe deine Antwort.

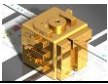
Ein Trojaner oder ein Computerwurm: ZIP-Dateien in Dateianhängen sind ein beliebter Weg, solche Schadprogramme zu verbreiten.

Ein Hörhinweis ist aufgenommen worden!

Von: WhatsApp +

ZIP 12abby x

Mein Freund



Authentisch oder nicht authentisch?

5. Überprüfe die E-Mail mit der bekannten Vorgehensweise auf Authentizität. Notiere die Ergebnisse.

Hinweise: Mit einem *HTML-Formular* (oder auch Webformular) können Daten erfasst und an einen Webserver gesendet werden.

Bei eBay haben Hacker vor einigen Jahren die kompletten Datensätze der Benutzer erbeutet. Durch das sofortige Ändern des Passwords kann zwar ausgeschlossen werden, dass die Kriminellen mit der Identität der Benutzer aktiv werden, die Daten sind aber im Umlauf.

eBay - **Käuferschutz !** Drucken Speichern Vollansicht

Von: eBay + 03.02.2015 um 03:59 Uhr

HTML formular x eBay <pruefung@eBay.de>

Hier war die korrekte Anrede mit Vorname und Name eingetragen

eBay - PayPal Käuferschutz Datenabgleich

Wenn Sie bei eBay einkaufen, sind Sie in sicheren Händen!

eBay KÄUFERSCHUTZ Mehr

Bei Bezahlung mit **PayPal**

Käuferschutz

Sehr geehrte/r ,

Hier war die korrekte Anrede mit Vorname und Name eingetragen

zur Sicherheit unserer Nutzer, insbesondere Ihres Nutzerkontos, ist es (aus Gründen des Käuferschutzes) erforderlich, dass wir Sie einer kurzen Legitimationsprüfung unterziehen.

Da es in der Vergangenheit vermehrt zu Missbrauchsfällen mit eBay-Nutzerkonten gab, möchten wir Sie darum bitten, Ihre Nutzerdaten über das angehängte Formular im Anhang zu validieren.

Die Validierung erfolgt vollautomatisch und dauert nur wenige Minuten.

WICHTIG: Sollten Sie die Legitimationsprüfung innerhalb der nächsten 5 Tagen nicht durchführen, so wird Ihr eBay-Nutzerkonto vorrübergehend eingeschränkt !

Ihre Hinterlegte Anschrift bei eBay !

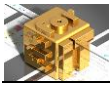
Hier war die komplette Postanschrift eingetragen

Mit freundlichen Grüßen,
eBay Kundenservice
Abt. Kontosicherheit

Klicken Sie auf die im E-Mail-Anhang angehängte Datei und klicken dann auf "Öffnen mit".

Tragen Sie Ihre Daten vollständig wie angegeben ein.

Sobald Ihre Daten Positiv überprüft worden sind, werden Sie zu unserer Startseite weitergeleitet.



- Abgleich der Absenderadresse mit dem E-Mail-Text.

Die Absenderadresse ist plausibel.

- Überprüfen der Grammatik und Rechtschreibung.

Grammatik und Rechtschreibung sind fehlerhaft.

- Klären der Notwendigkeit einer persönlichen Anrede.

Die persönliche Anrede ist korrekt.

Zusätzlich waren die Betrüger im Besitz der vollständigen Postanschrift.

- Internetrecherche mit Hilfe einer Suchmaschine nach einer prägnanten Formulierung, evtl. ergänzt um den Suchbegriff „spam“. Begriffe in Grafiken sind nutzlos.

Prägnant ist hier die fehlerhafte Formulierung „mit ebay nutzerkonten gab“.

Eine Suche liefert auch zutreffende Ergebnisse, z. B.:

„Was ist zur Zeit nur los? Gestern die täuschend echte PayPal Phishing Mail und heute ein zwar plumper, aber dennoch erschreckend authentischer eBay Phishing Versuch.

Diese Phishing Mail beinhaltet neben dem korrekten Namen auch die vollständige Anschrift des Empfängers – absolut erschreckend!“

(<https://www.phishing-mail.de/ebay-kaeuferschutz-phishing-mail-mit-kompletter-anschrift/>

Posted in eBay By Redaktion On August 29, 2014)

(Stand: September 2016)

- Suche nach Hinweisen auf Spam in dem Internetauftritt des angeblichen Anbieters. Verwende **nicht** den Link in der E-Mail, sondern öffne einen neuen Tab oder ein neues Fenster.

Auch bei eBay (<http://www.ebay.de/>) wird man fündig:

Über den Link „Hilfe – Fragen & Antworten“ führt die Suche nach „mit ebay nutzerkonten gab“ zu Treffern in „Antworten von der eBay-Community“.

- Wozu wird der Dateianhang vermutlich dienen?

Der Dateianhang dient hier **nicht** dem Zweck, ein Schadprogramm einzuschleusen.

Vielmehr dient es dem Phishing, indem der Benutzer dazu aufgefordert wird, seine Nutzerdaten bei eBay in das HTML-Formular einzugeben und an den Betrüger zu übermitteln.

➔ **Die E-Mail sollte sofort gelöscht werden.**