CHECKLISTE PHISHING

PHYSHING MAIL ENTARNT – Tipps vom Experten

RANSOMWARE

Hierbei handelt es sich um digitale Erpressung auf aller höchstem Niveau.

Mit nur einem falschen Klick, sind alle Daten futsch und unwiederbringlich verloren.

Jeder 3. Deutsche würde auf die Lösegeldforderung eingehen und für die Freilassung seiner Daten mehrere Hundert Euro an den Erpresser bezahlen.

Locky überfällt deutsche Internet-Nutzer mit bedrohlich klnigenden Phishing-Mails

Mehr als 5.000 PC werden pro Stunde von Locky erfolgreich überfallen und die Daten in Geiselhaft genommen.

BAUCHGEFÜHL UND SKEPSIS

Bevor Sie eine E-Mail Nachricht mit Anhang in Ihrem digitalen Posteingang öffnen, sollten Sie die Nachricht sorgsam prüfen.

Mit ein paar Tricks vom Experten erkennen Sie sofort ob es sich um eine „Fälschung“ handelt ?

Schauen Sie noch genauer hin!

Wenn Sie ein Tricks beachten, werden Sie verdächte E-Mails in Zukunft selbst identifizieren und Ihr System vor Viren wie Locky schützen.

Plausibilität Prüfung?
Kann die E-Mail eigentlich echt sein? Erwarte ich von diesem Absender überhaupt eine Nachricht. Habe ich tatsächlich etwas im Internet bestellt und ist das auch der korrekte Absender ?

Kann die Nachricht wirklich für mich persönlich sein?
Hat die Mail überhaupt eine korrekte Ansprache, oder ist Sie nur allgemein adressiert, mit „Sehr geehrte Damen und Herren“?

Ist die Mail auch wirklich an meine bekannte E-Mail-Adresse gerichtet?

Sind Schreibfehler in der Mail enthalten? Könnte das nicht auch eine Computer gestützte Übersetzung sein?

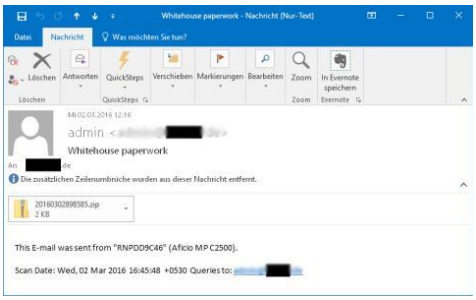
Bin ich überhaupt Kunde oder Mitglied, oder hatte ich überhaupt schon mal Kontakt mit dem vermeintlichen Absender?

Sehen Sie einmal genauer hin, kann es wirklich sein, das Sie etwas in dieser Summe im Internet in den letzten Tagen bestellt haben.

Ist der Anhang auch wirklich das, was er zu sein scheint, oder verbirgt sich dahinter ein gefährliches Archiv oder sogar ein ausführbares Programm?

„Lieber eine Mail zu viel gelöscht, als zu wenig.

Wenn jemand Ihnen etwas wichtiges zu sagen hat, wird er sich bestimmt noch einmal melden.



Prüfen Sie E-Mails mit Dateianhang besser zweimal auf Ihre Echtheit und Plausibilität

SICHERHEIT GEHT VOR

Wenn Sie in Eile sind und keine Zeit für die Analyse einer verdächtigen Mail haben, stellen Sie diese Aufgabe erst einmal zurück und kümmern Sie sich später darum.

Öffnen Sie niemals unbedacht einen Anhang einer E-Mail mit einem Doppelklick. Speichern Sie die Anlage erst auf Ihrem PC und sehen Sie sich mit der „rechten Maustaste“ zuerst einmal die Eigenschaften der Datei an.

Sollte es sich dabei um eine Anwendung (*.exe, *.bat, *.com, *.pif) handeln, löschen Sie die Datei sofort und auch die betreffende E-Mail.

Auch Archive (.zip oder .rar) sind sehr gefährlich, den darin befindet sich meist die Schadsoftware. Öffnen Sie die Archive nicht, sondern löschen Sie die Datei und die Mail sofort.

So erreichen Sie uns

ITSERVICE DORTMUND
Hagener Str. 241
44229 Dortmund
info@itservice-portal.de
www.ITService-Portal.de

- *Virenscan /Virenschutz*
- *Malware Bereinigung*
- *Einrichtung von Sicherungs-Plan*
- *Installation von Antivirus-Schutzsoftware*
- *Installation von Backup-Software*

GEFÄLSCHTE RECHNUNGEN

Leider sind auch harmlose Office Dokumente sehr verdächtig z.B. .xls (xlsx) oder .doc (docx). Aktuell wird der Locky-Virus als getarnte Rechnung in Form einer Excel-Tabelle versendet.

In der Excel-Tabelle selbst befindet sich meist der Schädling, oder wird beim Öffnen der Excel-Datei, aus dem Internet automatisch nachgeladen.

Sobald sich der Trojaner auf dem System eingenistet hat – unbemerkt – beginnt er mit dem Verschlüsseln sätlicher Dokumente, Tabellen, Bilder usw. Im gleichen Zuge sucht er nach weiteren PC im Netzwerk, die er dann auch infizieren wird.

Angebliche Rechnungen die sich in einem Archiv (.zip oder .rar) befinden sollten Sie ohne Kontrolle sofort löshen und niemals öffnen.

PRÜFEN SIE JEDE E-MAIL VOR DEM ÖFFNEN

Bevor Sie einen Link – egal wie bedrohlich dieser auch klingen mag – anklicken, stellen Sie die Maus einfach auf den Hyperlink und Sie sehen sofort ob die Ziel-URL auch tatsächlich zu dem Absender passt.

Obwohl die E-Mail anscheinend von dem Absender info@paypal.com zu kommen scheint und die links in der E-Mail aber nach http://paypal.sepa-umstellung.com zeigt, erkennen Sie sofort, dass es sich hierbei um eine Fälschung handelt.

Der Link müsste am Ende auf paypal.com zeigen, anderfalls ist das garantiert eine Fälschung! Wenn Sie unsicher sind ob Sie nicht tatsächlich eine Information von Paypal erhalten haben, klicken Sie – trotzdem nicht – auf den link in der E-Mail.

Öffnen Sie statt dessen einfach ein Browserfenster, mit Chrome, Firefox oder Internet-Explorer und geben Sie die URL www.paypal.de selbst ein. Nachdem Sie sich nun eingeloggt haben, werde Sie – sofern eine Information für Sie vorhanden ist – schon auf der Webseite auf eine wichtige Nachricht hingewiesen.

Auch beliebte Phishing Methoden sind E-Mails mit Anhang einer Rechnung, oder einer verzögerten Lieferung eines Paketes, oder auch mit einer Rückerstattung. In den meisten Fällen sind die Dateianhänge mit wichtigen Dateinamen tituliert und als getarntes ZIP-Archiv angehangen.

PHISHING MAIL

Der Ausdruck kommt aus dem Englischen und bedeutet so viel wie „etwas abfischen“.

Ziel ist es meistens geheime Informationen, wie Passwörter, Login-Daten und Zugangsdaten der Opfer ab zu fischen.

Dazu kopieren die Verbrecher die Internetseiten von Paypal, DHL, Banken und Mailanbieter um dem Opfer eine täuschend echte Webseite vor zu gaukeln.

Sofern das Opfer die präparierte Webseite besucht und sich einloggt werden die Daten abgefischt und dem Hacker zugänglich gemacht.

In vielen Fällen hat der Cyberdieb es aber nicht nur auf die persönlichen Daten abgesehen, sondern ist bestrebt seine Schadsoftware zu verbreiten.

Der infizierte Rechner ist mehr Wert, als die Zugangsdaten

Öffnen Sie so eine Rechnung – die als Archiv (ZIP oder RAR) in Ihrem Postfach ankommt, niemals mit einem Doppelklick.

Rechnungen und Angebote oder Auftragshinweise werden von allen seriösen Firmen heute als PDF-Dokument versendet. Diese erkennen Sie meistens an dem bekannten Acrobat-Icon.

Zip und Rar Archive erkennen Sie meist an diesem Symbol und sollten grundsätzlich erst einmal als gefährlich und verdächtig eingestuft werden.

Um sich vor den gefürchteten Ransomware zu schützen empfehlen wir folgende Sicherheitsmaßnahmen zu beachten:

- **Vorsicht bei E-Mail Anhängen:**

Sie sollten bei E-Mail s mit Anhängen – insbesondere Word und Excel oder Zip-Archive – sehr kritisch sein. Im Besten Fall löschen Sie die Nachricht sofort und öffnen unter keinen Umständen den Anhang.

- **Seien Sie kritisch auch bei Feunden**

Bei E-Mails von fremden Personen sollten Sie auch die Word oder Excel Anhänge nicht öffnen und einer strengen „Plausibilitäts-Prüfung unterziehen.

- **Lieferstatus und Rechnung per E-Mail?**

Gleiches sollten Sie auch bei angeblichen Rechnungen oder angeblichen Problemen mit einer Lieferung von unbekannten Firmen machen. E-Mails und Angebote werden üblicherweise im sicheren PDF-Format versendet und bestimmt nicht als Office-Dokument.

- **Software aktuell halten**

Betriebssystem und Browser und alle anderen wichtigen Programme – dazu zählt auch das Office und Outlook – sollten stets aktuell gehalten werden und die Sicherheitsupdates des Herstellers rechtzeitig eingespielt werden.

- **Windows und Office**

Sollten Sie noch keine Zeit für den Wechsel von Ihrem Windows-XP System gefunden haben, wäre jetzt ein guter Zeitpunkt das Betriebssystem auf die neue und sichere Version Windows 10, umzustellen. Ebenfalls sollten Sie ein Microsoft Office 2003 auch nicht mehr einsetzen und unbedingt auf eine aktuelle Version umsteigen.

- **aktueller Virenschutz ist Pflicht!**

ein abgelaufener Virenscanner bietet dem Verschlüsselungstrojaner und anderer Schadsoftware einen Zugang zu Ihrem System.
Deshalb sollten Sie Ihren Virenschutz immer aktuell halten und die Updates schnellstmöglich einspielen.
Verlangen Sie nicht von einem kostenlosen Scanner den gleichen Schutz wie Sie en von einer „bezahlten“ Software bekommen.

- **kein Lösegeld bezahlen**

Zahlen Sie unter keinen Umständen die Lösegeldforderung und folgen Sie auch nicht dem angebotenen link ins „Dark-Web“ um die Zahlungskonditionen auszuhandeln.

Bisher ist noch vollkommen unklar ob die Hacker auch wirklich in der Lage sind, die Verschlüsselung rückgangig zu machen.

In einer der letzten Varianten der Verschlüsselungtrojaner war es selbst dem Hacker nicht mehr möglich die „verschlüsselten Dateien“ wieder zu entsperren, da der Schlüssel vorsorglich gelöscht wurde.

In der Regel hat man das Lösegeld dann zu m Fenster herausgeworfen und die Daten bleiben mit einer AES 256Bit-Verschlüsselung für den User unbrauchbar.