- **Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.**

E-Mails vom Inkassobüro – alte Masche mit neuer Bedrohung!

Art der Bedrohung

Durch die Aktivierung der angehängten Schadsoftware kommt es mit höchster Wahrscheinlichkeit zu einer Verschlüsselung von Privat- und Firmendaten und der anschließenden Erpressung zur Bezahlung eines Geldbetrages mittels BitCoin´s!

Modus Operandi

Aktuell langen in der Meldestelle des C4 Mitteilungen über den Erhalt einer E-Mail ein, welche augenscheinlich von einem Inkassobüro stammt. Dabei wird der Empfänger persönlich angesprochen und ist auch eine entsprechende existente Anschrift (oder ehemaliger Wohnsitz) angeführt. Die E-Mail informiert über eine nicht bezahlte Rechnung bei einem (möglicherweise vor kurzem tatsächlich in Anspruch genommenen) online-Händler.

Die E-Mail selbst beinhaltet somit für den Empfänger nachvollziehbare Fakten und erscheint durchaus realistisch. Das angeführte Inkasso-Büro gibt es tatsächlich und bestätigte bereits zig-fache Anfragen von Personen welche diese E-Mail erhielten, steht aber selbst in keinem Zusammenhang mit der Massenaussendung.

Wird der angehängte Überweisungsträger „ausgedruckt“, startet dabei die Schadsoftware und es kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass es zu einer Verschlüsselung der Computer und/oder Netzwerkdaten kommt.

Bei der derzeit vorherrschenden Schadsoftware handelt es sich um so genannte Ransomware in den unterschiedlichsten Versionen. Für die Erlangung eines für die Entschlüsselung notwendigen Keys ist zumeist die Bezahlung von 1-3 BitCoin´s gefordert (1 BC = ~700,-, abhängig von starken täglichen Kursschwankungen).

Das vorliegende Phänomen war bereits 2008 stark vertreten, jedoch haben sich die Qualität der Schadsoftware und damit die Bedrohung potentiell erhöht (http://www.pctipp.ch/news/sicherheit/artikel/trojaner-vom-inkassobuero-45895/).

Empfohlene Vorgangsweisen:

- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen, insbesondere wenn sie angeblich von einem Inkassobüro stammen.
- Bevor Sie in solchen Mails angehängte Dateien öffnen oder Web-Links folgen, nehmen Sie telefonisch mit der zeichnenden Firma Kontakt auf und hinterfragen Sie die Anlagen.
- Sollte dies nicht möglich sein, öffnen Sie die Dateien nur in einer gesicherten Umgebung (virtuelle und wiederherstellbare Umgebung oder Sandbox) und auf nicht produktiven Geräten.
- Seien Sie bei der Bekanntgabe Ihrer persönlichen Daten vorsichtig, geben Sie niemals mehr als notwendig bekannt, übermitteln Sie keine Ausweiskopien. All diese Daten könnten für den Ursprung des nächsten Betruges zur Verwendung kommen.
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: http://www.bmi.gv.at.

Text und Grafik der E-Mail:

Gesendet: Montag, 05. Dezember 2016 um 01:55 Uhr
Von: " xxxxxxxxxx Inkasso xxxxxxxxxx"
An: "txxxxxxxxxx xxxxxxxxxx "
Betreff: Offene Forderung in Höhe von 183,25 EUR

Sehr geehrte/r Txxxxxxxxxx xxxxxxxxxx,

Da wir Sie an Ihrer Hausanschrift xxxxxxxxxx **Strasse xx** in xxxxxxxxxx über den Postweg nicht erreichen können, schreiben wir Ihnen nun eine E-Mail.

Sie haben aktuell eine offene Forderung in Höhe von

183,25 EUR

bei uns durch unbezahlte Rechnungen des Unternehmen xxxxxxxxxx **GmbH** offen.

Bitte schauen Sie sich die aktuelle Forderungsaufstellung an, drucken den beigefügten Überweisungsträger aus und überweisen Sie bitte den oben genannten Rechnungsbetrag an unser Bankkonto.

Wir setzen Ihnen eine Frist von **zwei Wochen**, um den offenstehenden Rechnungsbetrag an uns zu überweisen.
Sollten nach Ablauf der Frist kein Zahlungseingang festgestellt werden können, sind wir dazu beauftragt, gerichtliche Schritte gegen Sie einzuleiten.

Sollten Sie die offenstehende Rechnung bereits beglichen haben, so betrachten Sie diese E-Mail bitte als gegenstandslos.

Mit freundlichen Grüßen

Ihr Online-Team

xxxxxxxxxx Inkasso xxxxxxxxxx
xxxxxxxxxx xxxxxxxxxx
Tel +43 xxxxxxxxxx
Fax +43 xxxxxxxxxx
Mobil +43 xxxxxxxxxx

Weiterführende und erklärende Links:

Wikipedia – Ransomware: was ist Ransomware (https://de.wikipedia.org/wiki/Ransomware)

Watchlist-Internet –

- Inkassoforderungen von bekannten Unternehmen (https://www.watchlist-internet.at/sonstiges/inkassoforderungen-von-bekannten-unternehmen/)
- Neue Welle von betrügerischen Zahlungsaufforderungen (https://www.watchlist-internet.at/sonstiges/neue-welle-von-betruegerischen-zahlungsaufforderungen/)
- Tipps für sicheres Weihnachts-Shopping (https://www.watchlist-internet.at/sonstiges/tipps-fuer-sicheres-weihnachts-shopping/)

Bundeskriminalamt – Betrugsformen im Internet: (http://www.bmi.gv.at/cms/BK/betrug/start.aspx)

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG