CYBERCRIME COMPETENCE CENTER NEWS

INFORMATIONEN · TIPPS · RECHERCHEN · BERICHTE

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

E-Mails über angebliche Verkehrsstrafen – ACHTUNG: dahinter verbirgt sich Schadsoftware

Art der Bedrohung

Beschädigung oder Verschlüsselung von Privat- und Firmendaten und anschließende Erpressung zur Bezahlung eines Geldbetrages mittels BitCoin zur Erlangung des Entschlüsselungs-Codes / Programms

Modus Operandi

Nach den angeblichen Bewerbungsschreiben, Rechnungen vom Verbund, Finanzamt oder Zustellern wie DHL und Post, welche zu zahlreichen Datenverschlüsselungen führten, wird derzeit scheinbar eine neue Masche für die Zusendung der Schadsoftware durch die Täter vorbereitet.

Im vorliegenden Falle werden E-Mails mit dem Betreff „Fotofixierung des Verkehrtsunfalls #725-1205“, welche angeblich von der Kantonspolizei (angezeigter Name) stammen, zugestellt. Die tatsächliche Absenderadresse lässt jedoch keine Rückschlüsse auf den Versand durch eine Behörde zu (Bild 1).

Der E-Mail ist ein Word-Dokument mit dem Namen „Strafe.docx“ sowie ein gepackte Datei Namens „Fotofixierung.zip“ angehängt.

Wird die Word-Datei geöffnet erscheint ein Foto sowie der Hinweis, dass für die Vollanzeige des Bildes zweimal auf dieses geklickt werden muss. Achtung! Dabei wird über ein Script versucht Schadcode aus dem Internet nachzuladen und zu installieren (Bild 2).

Bei der derzeit im Umlauf befindlichen E-Mail dürfte es sich (noch) um eine Teststellung oder mangelhafte Version handeln, da die eigentliche (nachzuladende) Schadsoftware durch das Script auf dem System nicht vorgefunden und installiert werden konnte (Bild 3).

Erfahrungsgemäß ist jedoch davon auszugehen, dass eine entsprechend adaptierte Version der E-Mail mit der angeblichen „Strafe nach Verletzung der Straßenverkehrsordnung“ in absehbarer Zeit als Massen-E-Mail versendet wird.

Bedenken Sie bitte, dass Ihnen weder eine Behörde noch ein Strafamt auf diese Art und Weise eine Vorschreibung zusenden würde!

Empfohlene Vorgangsweisen:

- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen oder wenn Sie keine entsprechenden Mitteilungen erwarten.
- Kontrollieren Sie nach Möglichkeit die tatsächliche Absenderadresse, achten Sie auf Ungereimtheiten. Bei angeführten Weblinks legen Sie den Mauszeiger über den entsprechenden Link, ohne diesen zu aktivieren. Sollte die Web-Link-Adresse aufscheinen, kontrollieren Sie, ob diese tatsächlich zum Absender gehört.
- Achten Sie auf die Schreibweise und Rechtschreibung solcher Nachrichten, Täter verwenden hier gerne Übersetzungsprogramme, wodurch der Betrug leicht erkennbar ist.
- Öffnen Sie keinesfalls Ihnen unbekannte Dateianhänge, ohne sich vorher von deren „Echtheit“ zu überzeugen. Werden Ihnen Bewerbungsunterlagen zum Download „angeboten“, tun Sie dies bitte nicht! Wenn Sie dennoch der Ansicht sind, dass es sich um echte und notwendige Dokumente handelt, laden Sie die Datei nur in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) und auf nicht produktiven Geräten herunter und öffnen diese dann auch dort. Oder bedienen Sie sich unterstützender Seiten im Internet (z.B. Virustotal.com).
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Legen Sie sich eine BackUp-Strategie für Ihre Daten zu. Trennen Sie das BackUp-Medium nach der Sicherung vom System und lösen Sie Share-Links zu BackUp Servern nach erfolgter Sicherung wieder auf, um ein Übergreifen durch die Schadsoftware zu verhindern.
- Beschränken Sie die Benutzerrechte der jeweiligen User so weit als möglich und arbeiten Sie nur unter dem Administrator-Account, wenn dies unbedingt notwendig ist.
- Wir raten den geforderten Betrag nicht zu bezahlen, es sei denn, dass die Wiederherstellung der Daten für Sie unumgänglich ist. Eine Garantie auf eine solche, selbst nach Bezahlung, gibt es nicht, jedoch liegt es im „Geschäftsmodell“ der Täter, einer solchen nachzukommen! Eine letztendliche Entscheidung darüber müssen Sie für sich selbst treffen.
- 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.

Bild 1:

Von: Kantonspolizei [mailto:info@gloor-sieger.ch]
Gesendet: Montag, 26. Juni 2017 12:44
An: [redacted]
Betreff: Fotofixierung des Verkehrtsunfalls #725-1205

Guten Tag,

Sie haben die Strassenverkehrsordnung verletzt.

Fotobestätigung und detaliierte Information über die Strafe werden beigelegt.

Bild 2:

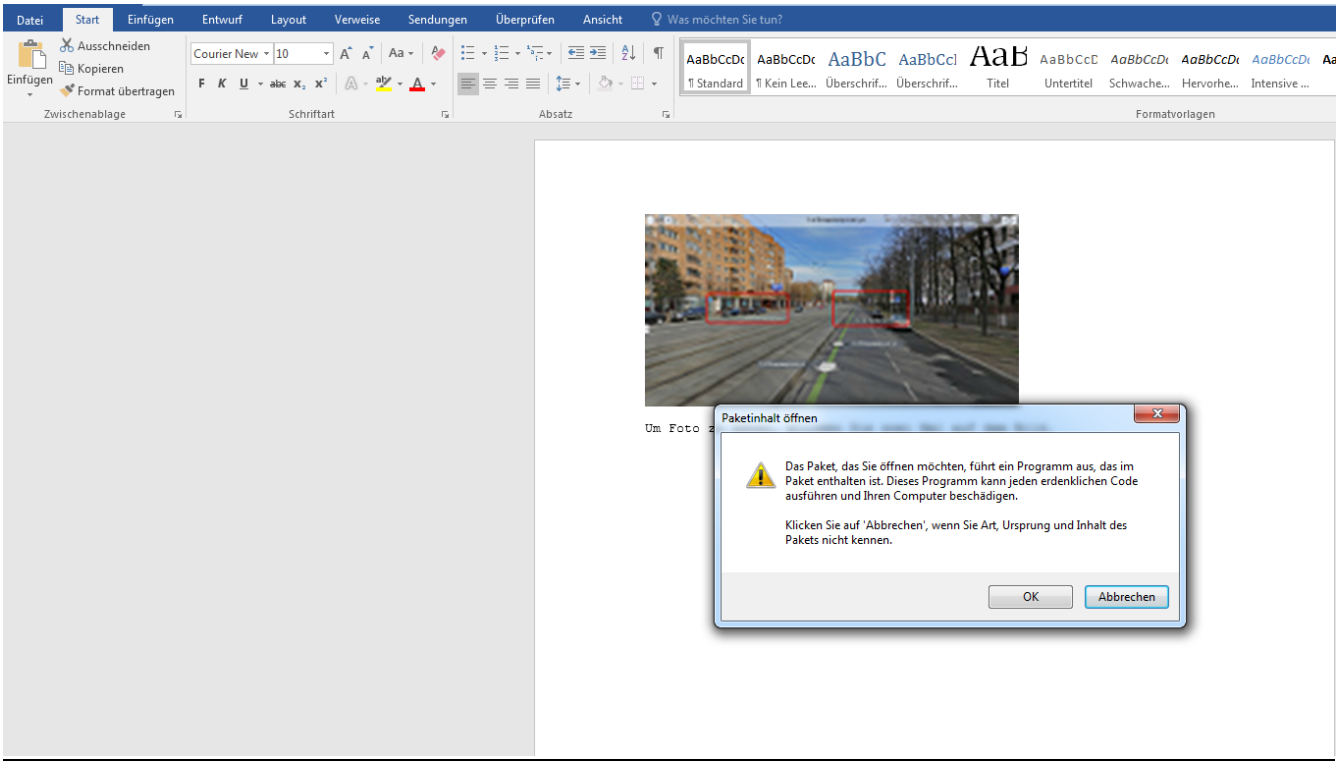
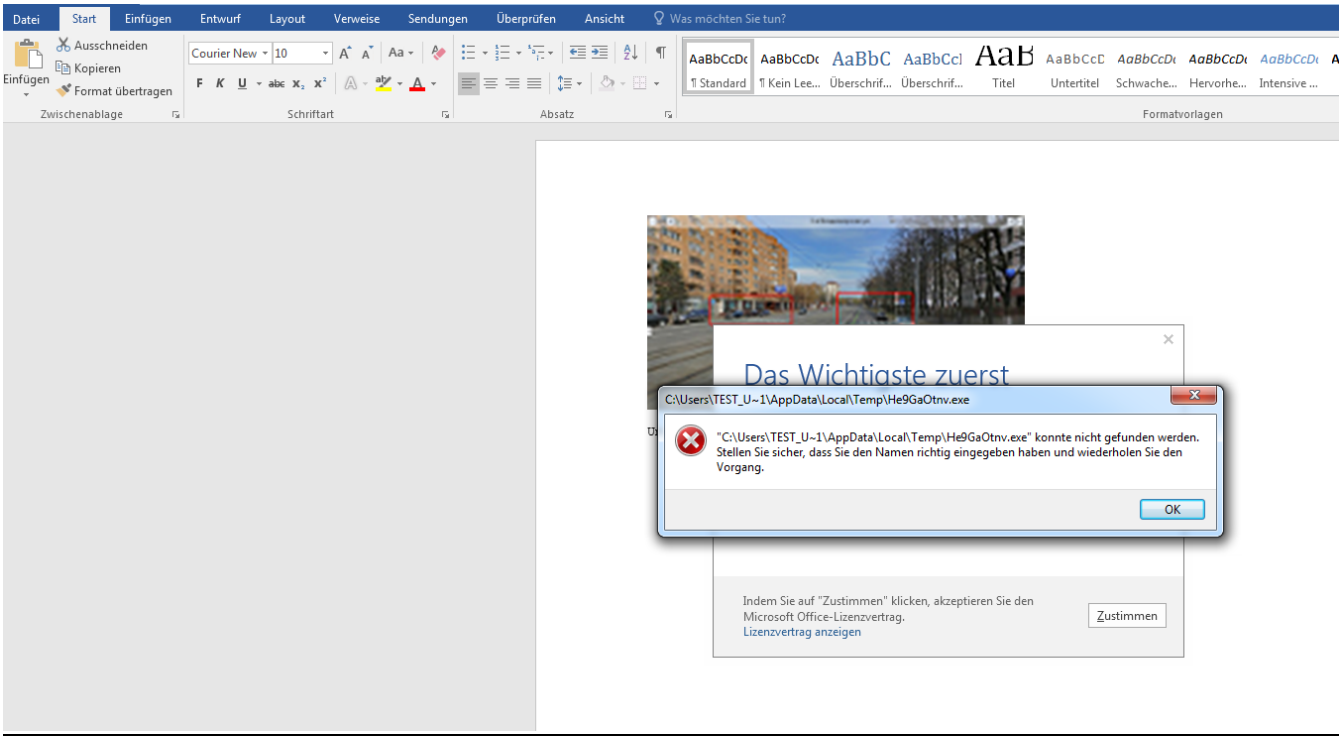

Datei
Start
Einfügen
Entwurf
Layout
Verweise
Sendungen
Überprüfen
Ansicht
Was möchten Sie tun?
Ausschneiden
Kopieren
Format übertragen
Einfügen
Courier New
10
Zwischenablage
Schriftart
Absatz
Formatvorlagen
Um Foto
Paketinhalt öffnen
Das Paket, das Sie öffnen möchten, führt ein Programm aus, das im Paket enthalten ist. Dieses Programm kann jeden erdenklichen Code ausführen und Ihren Computer beschädigen.
Klicken Sie auf 'Abbrechen', wenn Sie Art, Ursprung und Inhalt des Pakets nicht kennen.
OK
Abbrechen

Bild 3:


Datei
Start
Einfügen
Entwurf
Layout
Verweise
Sendungen
Überprüfen
Ansicht
Was möchten Sie tun?
Ausschneiden
Kopieren
Format übertragen
Einfügen
Courier New
10
Zwischenablage
Schriftart
Absatz
Formatvorlagen
Das Wichtigste zuerst
C:\Users\TEST_U~1\AppData\Local\Temp\He9GaOtnv.exe
"C:\Users\TEST_U~1\AppData\Local\Temp\He9GaOtnv.exe" konnte nicht gefunden werden. Stellen Sie sicher, dass Sie den Namen richtig eingegeben haben und wiederholen Sie den Vorgang.
OK
Indem Sie auf "Zustimmen" klicken, akzeptieren Sie den Microsoft Office-Lizenzvertrag.
Lizenzvertrag anzeigen
Zustimmen

Weiterführende und erklärende Links:

Technische Analyse der Datei „Strafe.docx“ auf malwr.com:
https://malwr.com/analysis/OTFmYmJjMjU5YTBmNGMxMjg2MWRlNmFlOTE5ZDI2OTg/#

No More Ransom Projekt: Initiative zur Wiederherstellung von Daten nach Angriffen mit Ransomware (https://www.nomoreransom.org/)

Bundeskriminalamt Wien: http://www.bmi.gv.at/cms/BK/wir_ueber_uns/start.aspx

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

FEEDBACK

NEWSLETTER AN-/ABMELDUNG