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

Angebliches Rechnungsschreiben vom Energieanbieter Verbund per E-Mail macht Ihre Daten durch Verschlüsselung unbrauchbar

Art der Bedrohung

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

Modus Operandi

Aktuell ist eine neue Welle von Mails mit gefährlichem Inhalt unterwegs. Nunmehr gibt die Mail vor vom Energieanbieter „Verbund Österreich“ zu stammen und gibt Ihnen die Möglichkeit aufgrund der dargestellten Rechnungsübersicht, sich die „online“-Rechnung ansehen zu können.

Bei dem über einen blauen Balken in der Mail zu öffnenden Link wird man auf eine Webseite weitergeleitet, auf welcher die „Rechnung“ als ZIP-Datei zum Download bereit steht. Darin verbirgt sich ein getarntes JavaScript, welches nach Aktivierung die entsprechende Schadsoftware nachlädt. Von der Schadsoftware werden Benutzerdaten auf dem lokalen System, verbundene Server-Shares sowie angeschlossene, beschreibbare USB-Laufwerke durch die Ransomware „Crypt0L0cker“ verschlüsselt. Für den Erhalt des für die Entschlüsselung notwendigen „Key´s“ ist die Bezahlung eines „Lösegeldes“ (Ransom) mittels BitCoin erforderlich. Die Anweisungen für die Kontaktaufnahme erfolgen auf dem Bildschirm des Benutzers.

Da nahezu jeder Haushalt und jede Firma in Österreich Energie-Konsument ist und tatsächlich zahlreiche Firmen auf die online-Rechnung umsteigen oder damit werben, erscheint die derzeitige Zusendung als äußerst plausibel und wird gerade im Firmen und Geschäftsbereich als tatsächliche Forderungsmitteilung angesehen. Tatsächlich steht natürlich Verbund Österreich in keinem Zusammenhang mit den versandten E-Mails und warnt bereits auch auf seiner Webseite und auf Facebook vor derartigen E-Mails.

Wir raten derart geforderte Zahlungen nicht zu leisten. Die Bezahlung sollte das allerletzte Mittel sein, wenn Sie auf die verschlüsselten Daten keinesfalls verzichten können. Besser beraten sind Sie, wenn Sie zeitgerecht die finanziellen Mittel in eine entsprechende BackUp-Lösung und Strategie investieren.

Eine Wiederherstellung oder Entschlüsselung der Daten ohne den erforderlichen „Key“ ist auf Grund

der hohen Qualität der Verschlüsselung derzeit nahezu unmöglich.

Zudem können unter Umständen von der Schadsoftware in der Windows-Registry gespeicherte Zugangsdaten und Passwörter, unter anderem für FTP und E-Mail-Accounts ausgelesen und per Mail an eine vom Täter adressierte Stelle im Internet versandt werden. Bei neueren Versionen der Schadsoftware erfolgt ebenfalls zu diesem Zeitpunkt die Löschung der sog. „Shadow Copy", welche bei Vorversionen dieser Schadsoftware in manchen Fällen noch eine Teilwiederherstellung der Daten zuließ.

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.
- Wenn Sie sich unsicher sind, öffnen Sie derartige Dateien in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) 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.

Text und Grafik der E-Mail, welche über die Rechnung informiert:

VERBUND

Detailaufstellung zu Rechnung Nr. 542975954

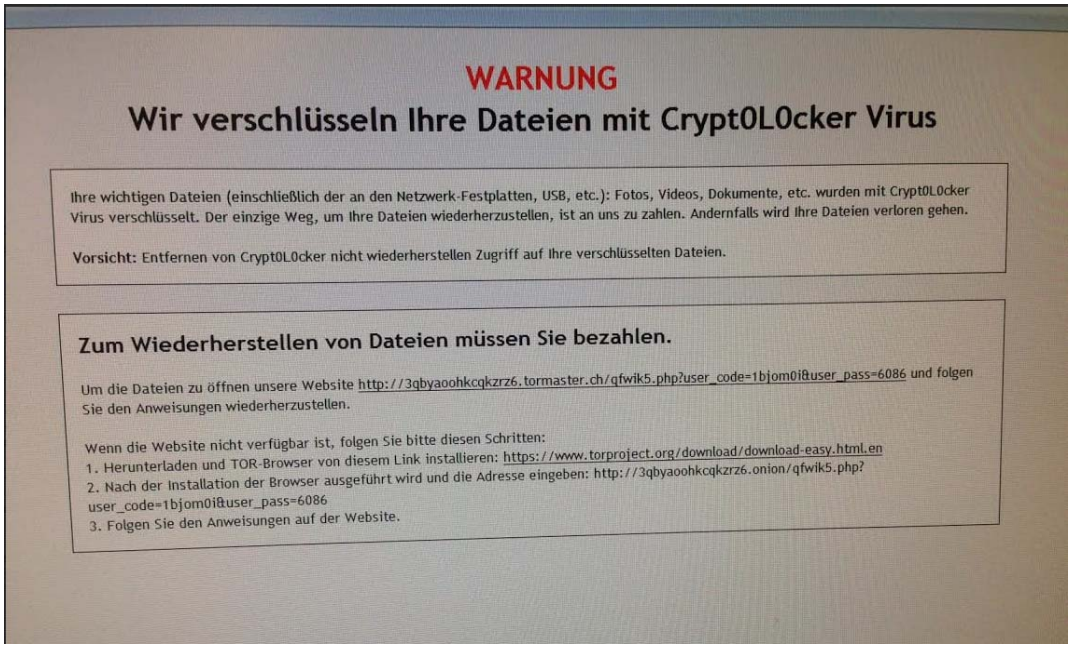
Kundennummer:	30178553
Anlagennummer:	64203266
netztarif:	Netzebene 7, Wien, nicht gemessene Leistung
Ausmaß der Netznutzung:	4,00 kW
Energiekosten gesamt:	**212,73 €**

Ansicht einer Rechnung

Eine Abrechnung Ihrer Energieeinspeisung werden wir dann durchführen, wenn wir die dafür erforderlichen Daten von Ihrem Netzbetreiber erhalten. Die Zahlung unterliegt der Besteuerung nach Maßgabe der Rechnungslegung gemäb § 17 UstG.

VERBUND	Privatkunden	Geschäftskunden
Mediathek / Pressefotos Ungeplante Kraftwerksausfälle Konzerneinkauf / Lieferanten Kunstsammlung	Ihr Stromprodukt von VERBUND Strom aus Wasserkraft Klimaneutrales Gas von VERBUND Alles rund um Photovoltaik	Energie für Ihr Gewerbe Strom: Angebot für KMU Stromlösungen für Industriekunden Energieversorger

Nach der Verschlüsselung erscheint die Aufforderung zur Bezahlung:



Weiterführende und erklärende Links:

Wikipedia – CryptoLocker (englisch): was ist CryptoLocker und dessen Geschichte (https://en.wikipedia.org/wiki/CryptoLocker)

Wikipedia – BitCoin: die Entstehung und Entwicklung der „digitalen Münze“ (https://de.wikipedia.org/wiki/Bitcoin)

Watchlist-Internet – Falsche Verbund-Rechnung: Aufbereitung und Warnung vor dem gegenständlichen Phänomen (https://www.watchlist-internet.at/gefaelschte-rechnungen/falsche-verbund-rechnung-verbreitet-schadsoftware/)

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

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

FEEDBACK

NEWSLETTER AN-/ABMELDUNG