Was tun bei einem Verdacht?

- Senden Sie die erhaltene E-Mail keinesfalls weiter, da sich so der Virus verbreitet.
- **Fotografieren** Sie falls möglich den Bildschirm samt der Erpresser-Nachricht oder notieren Sie die Ausschriften.
- Ziehen Sie den Netzstecker oder fahren Sie den PC sofort herunter.
- Informieren Sie Ihren IT-Betreuer oder den IT-Service über den Vorfall.
- Gehen Sie nicht voreilig auf **Lösegeldforderungen** ein, denn die Dateien und Programme werden oftmals trotz der Bezahlung nicht entschlüsselt.
- Setzen Sie falls möglich Ihr System neu auf und stellen Sie Ihre Daten aus einem Backup wieder her.

Quellen und weiterführende Informationen

Detaillierte Informationen zum Thema Phishing und Ransomware erhalten Sie im Universitätsrechenzentrum der Friedrich-Schiller-Universität Jena.

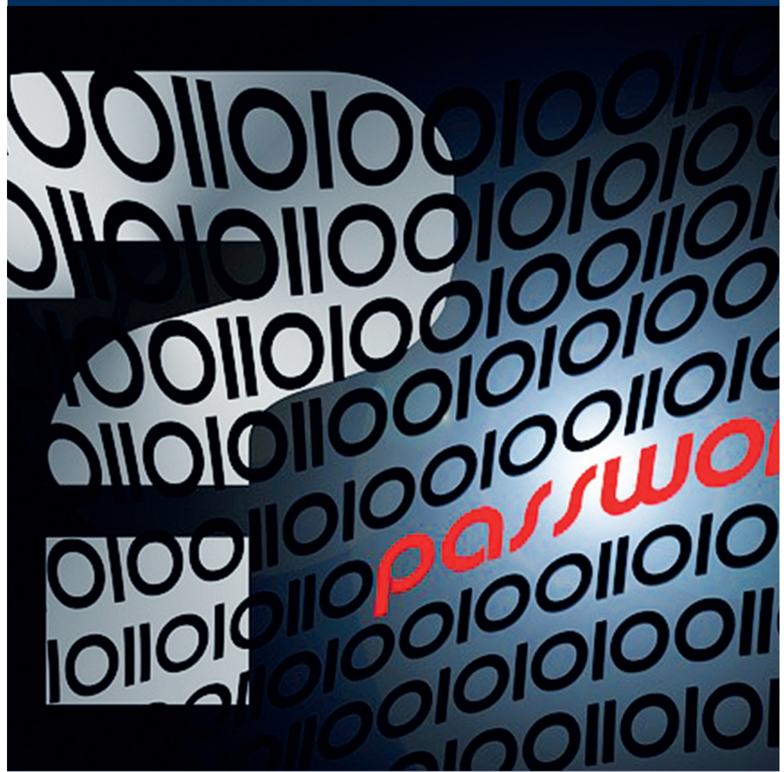
Folgende Quellen wurden einbezogen:

- SOPHOS – Security made simple
- Klopfer Datennetzwerk GmbH
- Bundesamt für Sicherheit in der Informationstechnik

Kontakt

Universitätsrechenzentrum
Stabsstelle Sicherheit Informationstechnischer Systeme
Am Johannisfriedhof 2
07743 Jena
Telefon: +49 3641 9-40515
E-Mail: st-sis@uni-jena.de
Internet: http://www.uni-jena.de/st_sis

IMPRESSUM
Friedrich-Schiller-Universität Jena, Universitätsrechenzenrtum,
Am Johannisfriedhof 2, 07743 Jena | Satz und Druck: Druckzentrum
Stand: Februar 2016



Phishing und Ransomeware

Verhalten bei Sicherheitsvorfällen

Friedrich-Schiller-Universität Jena

Ransomware

Ransomware ist eine **Schadsoftware**, die Daten oder den gesamten PC als Geisel nimmt und diese verschlüsselt (auch als Cryto-Trojaner bezeichnet). Ziel dabei ist es, Lösegeld (engl. Ransom) zu erpressen.

Dies ist sehr ernst zu nehmen, da dieses Problem sowohl Unternehmen als auch Privatpersonen gleichermaßen betreffen kann.

Einschleusen

1. Die schädliche Software gelangt meist durch E-Mail-Anhänge auf die Geräte – **„Phishing“**. Sobald die infizierten Anhänge geöffnet werden, startet im Hintergrund die Installation. Es kann dazu kommen, dass von befallenen Rechnern automatisch E-Mails an das gesamte Adressbuch gesendet werden. Somit stammen die Mails nicht immer von unbekannten Absendern.
2. Auch **gefälschte Rechnungen** von Dienstleistern werden häufig als Falle genutzt. Es ist deshalb zu empfehlen, keine Nachrichten von unbekannten Absendern zu öffnen.
3. Ein weiterer Weg sind **kompromittierte Webseiten**: Nur durch das Aufrufen einer Webseite im Browser wird automatisch und unbemerkt die schädliche Software installiert. Bei zweifelhaften Links ist somit Vorsicht geboten.

Merkmale

Folgende Anzeichen können auf eine **Infektion durch Schadprogramme** hinweisen:

- Probleme beim Starten des PC's
- unerwartete Netzzugriffe
- unerklärliche Veränderungen von Datei-Inhalten
- nicht auffindbare Dateien
- Probleme beim Verändern oder Abspeichern von Dateien
- häufige Abstürze von Programmen
- unerklärliche Fehlermeldungen
- Versand von E-Mails ohne Aktion des Benutzers
- kein Zugriff auf einzelne Laufwerke oder Datenträger
- ständige Verringerung des freien Speicherplatzes, ohne dass etwas gespeichert wurde

Schutz vor Übergriffen

Zwar gibt es keinen hundertprozentigen Schutz vor derartigen Übergriffen, dennoch können Sie einige **Hinweise** befolgen, um eine Infizierung Ihres Gerätes zu vermeiden:

- Sorgen Sie für **regelmäßige Backups**, um im Schadensfall eine Rücksicherung der Daten zu gewährleisten.
- Sichern Sie Ihre Daten regelmäßig auf einem **externen Speichermedium**, zum Beispiel einer USB-Festplatte. Diese sollte jedoch nicht dauerhaft mit Ihrem Rechner verbunden sein.
- Bewahren Sie Ihre Datensicherung **getrennt** von Ihrem Rechner auf. So sind Ihre Daten auch im Brandfall oder anderen Katastrophen geschützt.
- Prüfen Sie, ob sich die gesicherten Daten auch tatsächlich **wiederherstellen** lassen.
- Aktivieren Sie die **Firewall Ihres PC's**, da diese bereits einen großen Teil schädlicher Daten abfängt.
- Installieren Sie einen **aktuellen Virenschutz** und sorgen Sie dafür, dass er immer auf dem neusten Stand ist. Eine Variante wäre das Installationspaket des Virenschutz **„Sophos“** der Universität Jena.
- Spielen Sie regelmäßig die **Sicherheitsupdates** für Betriebssystem und Anwendungsprogramme auf, um eventuelle Lücken in den Programmen für die Trojaner zu schließen.
- Seien Sie **wachsam und misstrauisch**. Überprüfen Sie die Herkunft unbekannter E-Mail-Adressen und fragen Sie gegebenenfalls bei der Firma nach. Links verweisen oftmals auf dubiose Seiten. Achten Sie darauf besonders.