Schutz vor Phishing

Zusammenfassung

Hier stehen die wichtigesten Informationen zum Thema "Phishing" und dem Verhalten bei einem Sicherheitsvorfall zur Verfügung.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**
- **Gäste der Friedrich-Schiller-Universität**

Erkennen von und Verhalten bei Empfang von Phishing-E-Mails

Flyer zum Thema Phishing	Flyer zum Thema Ransomware	Anleitung zur Dekativierung v

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 zunehmen, 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.
4. Es werden gern **beunruhigende Situationen** des Alltagslebens genutzt, um Nutzer zu Klicken auf einen Link zu bewegen.

Aktuelles Beispiel dafür ist die Corona-Krise.
Niemand kann einen seriösen Test oder gar Schnelltest verkaufen, einen einhundertprozentigen Schutz vor Infektion bieten oder wirksame Mittel nennen, die man nicht bereits aus seriösen Quellen kennt. Mögliche Inhalte dieser E-Mails findet man hier.

Merkmale

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

- Probleme beim Starten des PC‘s
- unerwartete Netzzugriffe
- unerklärliche Veränderungen von Dateiinhalten
- nicht auffindbare Dateien
- Probleme beim Verändern oder Abspeichern von Dateien
- häufige Abstürze von Programmen
- unerklärliche Fehlermeldungen
- Versand von E-Mails ohne Aktion des Benutzers/der Benutzerin
- 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 kann man einige **Hinweise** befolgen, um eine Infizierung des Gerätes zu vermeiden:

- Für **regelmäßige Backups sorgen**, um im Schadensfall eine Rücksicherung der Daten zu gewährleisten.
- Regelmäßiges Sichern der Daten auf einem **externen Speichermedium**, zum Beispiel einer USB-Festplatte. Diese sollte jedoch nicht dauerhaft mit dem Rechner verbunden sein.
- Die Datensicherung **getrennt** vom Rechner aufbewahren. So sind die Daten auch im Brandfall oder anderen Katastrophen geschützt.
- Prüfen, ob sich die gesicherten Daten auch tatsächlich **wiederherstellen** lassen.
- Die **Firewall des PC‘s aktivieren**, da diese bereits einen großen Teil schädlicher Daten abfängt.
- Einen **aktuellen Virenschutz** installieren und und dafür sorgen, dass er immer auf dem neusten Stand ist. Eine Variante wäre das Installationspaket des Virenschutz „**Sophos**“ der Universität Jena.
- Regelmäßig die **Sicherheitsupdates** für Betriebssystem und Anwendungsprogramme installieren, um eventuelle Lücken in den Programmen für die Trojaner zu schließen.
- **Wachsam und misstrauisch sein**. Die Herkunft unbekannter E-Mail-Adressen überprüfen und gegebenenfalls bei der Firma nachfragen. Links verweisen oftmals auf dubiose Seiten.

Was tun bei einem Verdacht?

- Die erhaltene E-Mail keinesfalls weitersenden, da sich so der Virus verbreitet.
- Den Bildschirm samt der Erpresser-Nachricht möglichst fotografieren oder notieren die Ausschriften notieren.
- Den Netzstecker ziehen oder den PC sofort herunterfahren.
- D IT-Betreuer oder den IT-Service über den Vorfall informieren.
- Nicht voreilig auf **Lösegeldforderungen** eingehen, denn die Dateien und Programme werden oftmals trotz der Bezahlung nicht entschlüsselt.
- Das System neu installieren und die Daten aus einem Backup wiederherstellen.

Neuer Service zur Meldung von verdächtigen Phishing-E-Mails

Aus gegebenen Anlass und den immer wiederkehrenden Angriffen auf Studentinnen/Studenten und Mitarbeiterinnen/Mitarbeiter der Universität Jena möchten wir über unsere neue Phishing-Mail-Adresse informieren.
Wenn man eine E-Mail bekommen und diese als Betrugsversuch erkannt hat oder man sich wegen eines möglichen Phishing-Versuchs unsicher ist, dann sollte man weder auf Links klicken noch Dateianhänge öffnen oder auf die E-Mail antworten. Mit einer Antwort auf Phishing-E-Mails bestätigt man die Existenz und Aktivität des E-Mail-Kontos.
Immer nachfragen! Auch bei bekannten und vertrauten Personen!
Im Verdachtsfall solche E-Mails an phishing@uni-jena.de weiterleiten. Eine automatische Rückantwort wird generiert. Ab jetzt erfolgt die Verarbeitung des Inhalts der weitergeleiteten E-Mail automatisch, sodass nach dieser E-Mail keine weiteren Antworten gesendet werden.

Sollte die Analyse ergeben, dass:

- die E-Mail LINKS zu gefälschten Webseiten enthält, so werden diese im Universitätsnetz vorübergehend gesperrt,
- die E-Mail eine gefälschte Absender-ADRESSE enthält, die auf "...@uni-jena.de" endet, so wird das zugehörige Nutzerkennzeichen vorübergehend gesperrt. Sollte die gefälschte Absender-ADRESSE nicht auf "...@uni-jena.de" enden, so können wir keine Sperrung durchführen.

Quellen und weiterführende Informationen

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

Folgende Quellen wurden einbezogen:

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