Landeskriminalamt
Cyber Competence Center
ZAC - Zentrale Ansprechstelle
Cybercrime für die Wirtschaft

Die Zentrale Ansprechstelle Cybercrime (ZAC) informiert:

Digitale Erpressung - Schutz vor Ransomware

Die Zentrale Ansprechstelle Cybercrime (ZAC) des LKA Brandenburg erreichen immer öfter Anfragen von betroffenen Firmen und Behörden zur aktuellen Verbreitung der „Krypto-Ransomware“ und zum Umgang mit den durch Schadsoftware infizierten Computersystemen. Dabei spielen sowohl allgemeine Fragen als auch der Umgang mit aktuellen Ransomware-Phänomen (z. B. „Goldeneye“) eine Rolle. Die aktuellen Verschlüsselungstrojaner verbreiten sich vornehmlich in E-Mails, die getarnt z. B. als Bewerbung auf offene Stellenausschreibungen, derzeit vor allem Firmen und Behörden erreichen. Diese „Bewerbungen“ sind in fehlerfreiem Deutsch geschrieben und enthalten meist ein Lichtbild des angeblichen Bewerbers. Angehängt an diese E-Mails befinden sich die vermeintlichen Bewerbungsunterlagen in Form einer Excel-Datei (.xls) sowie einer PDF-Datei.

Sogenannte „Ransomware-Schadprogramme“ sind in einer Vielzahl an Varianten bereits seit mehreren Jahren im Umlauf. Eine dieser neueren Varianten ist die sogenannte „Krypto“-Ransomware. E-Mails mit dieser Schadsoftware sind getarnt als Rechnung, Paketankündigung, Bewerbungsschreiben oder als gewerbliches Angebot. *„Heute sind es Stellenausschreibungen, in der nächsten Woche vielleicht was ganz anderes. Seien Sie deshalb kritisch beim Öffnen von Dateianhängen und sorgen Sie für eine aktuelle Virensoftware auf ihrem PC.“*.

Diese Schadsoftware verschlüsselt beim Öffnen des Dateianhangs oder anklicken eines Links das Computersystem oder ganze Netzwerke. Bei den angehängten Dateien handelt es sich beispielsweise um zip-Formate, exe-Dateien oder als Makros programmierte Word- oder Excel-Dateien in Microsoftprodukten. Der Geschädigte wird meist mittels einer Textdatei über die Datenverschlüsselung seines Systems informiert und zu einer Lösegeldzahlung aufgefordert, um den Computer wieder freizuschalten.

Zum Schutz vor einer Infizierung mit „Ransomware“ gibt die ZAC Brandenburg folgende Handlungshinweise:

- Scannen Sie ein- und ausgehende E-Mails auf Malware und entfernen Sie ausführbare Dateien.
- Nutzen Sie Spam-Filter, sodass möglichst wenig unerwünschte Mails den Endnutzer erreichen.
- Verhindern Sie durch Ihren E-Mail-Server die Annahme externer Mails mit internem Absender.
- Verhindern Sie die Ausführung aktiver Inhalte in E-Mails und Office-Dokumenten oder erlauben Sie deren Ausführung erst nach ausdrücklicher Bestätigung des Nutzers.
- Nutzen Sie für die E-Mail-Kommunikation (sowohl intern als auch extern) digitale Zertifikate/ Signaturen um Absender zu verifizieren und die Manipulation von Nachrichten zu verhindern.
- Blockieren Sie durch Ihre Firewall Zugriffe auf verdächtige IP-Adressen und Domains.
- Überprüfen Sie durch einen Virenschutz in regelmäßigen Abständen Ihre Systeme. Häufig wird die Schadsoftware erst zu einem späteren Zeitpunkt durch aktualisierte Virensignaturen erkannt. Durch die Nutzung proaktiver Schutzmechanismen (beispielsweise cloudbasierte Analysen oder Verhaltensanalyse) kann die Erkennungsrate der Antivirensoftware verbessert werden. Aktualisieren Sie ihre Schutzsoftware regelmäßig.
- Deinstallieren Sie nicht benötige Software und führen Sie regelmäßige Updates für die eingesetzten Softwareprodukte und Betriebssysteme durch. Ein zentrales Patch-Management kann hierbei hilfreich sein.

Falls es dennoch zum Schadenfall kommt:

- Trennen Sie unverzüglich die Netzwerkverbindung von infizierten Rechnern.
- Schalten Sie betroffene Geräte umgehend aus, um die Verschlüsselung weiterer Daten zu verhindern.
- Isolieren Sie Backups, damit diese nicht ebenfalls verschlüsselt werden.

- Sichern Sie relevante Dateien, die Aufschluss über den Infektionshergang geben können. Hierzu zählen beispielsweise Log-Dateien oder E-Mails.
- Ändern Sie sämtliche Benutzer- und Netzwerkkennwörter, sofern diese durch den Vorfall kompromittiert sein könnten.
- Erstatten Sie Strafanzeige bei der Polizei!

Kontakt & Information: ZAC - Zentrale Ansprechstelle Cybercrime für die Wirtschaft und Behörden im Land Brandenburg: Partner für Informationen zur Vermeidung von Cybercrime-Angriffen als auch bei Ermittlungen zu qualifizierten Cybercrime-Straftaten gegen Firmen und Behörden
Tel. 03334 388-8686, E-Mail: ZAC@polizei.brandenburg.de
- außerhalb der Bürodienstzeit: Tel. 0331 283-3035 / Fax. - 3059 (Einsatz- und Lagezentrum des Polizeipräsidiums)

Links

- BSI: Lagedossier Ransomware vom 07.07.2016
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lagedossiers/Lagedossier_Ransomeware.html
- BSI: Ransomware - Bedrohungslage, Prävention & Reaktion vom 11.03.2016
  https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Ransomware_11032016.html
- BKA: Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime
  http://www.bka.de/nn_238144/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html
- Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime der Länder und des Bundes
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/.../ZAC/polizeikontakt.html