Cybersicherheitsagentur Baden-Württemberg
(CSBW)

Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: Ransomware

Ransomware = Schadsoftware, um Lösegeld zu erpressen

Eine der größten Bedrohungen der Cybersicherheit stellen Ransomware-Angriffe dar. Für Cyberkriminelle ist dies ein finanziell äußerst lukratives Geschäftsmodell, da durch Erpressung in kurzer Zeit hohe Geldsummen erbeutet werden können. Besonders gefährlich macht Ransomware, dass es alle treffen kann, die online unterwegs sind.

Was ist Ransomware?

Ransomware wird auch als Verschlüsselungstrojaner oder Erpressersoftware bezeichnet.

Der Begriff Ransomware setzt sich aus „ransom“ (dt. Lösegeld) und „software“ (dt. Programm) zusammen. Dementsprechend handelt es sich bei Ransomware um ein Schadprogramm, das zur Erpressung von Lösegeld genutzt wird.

Angreifende verschlüsseln mit Hilfe eines Schadprogramms Daten und Systeme, sodass Nutzende darauf keinen Zugriff mehr haben. Insbesondere für Verwaltungen und Unternehmen kann dies mit großen Schäden verbunden sein. Aber auch Privatpersonen können von Ransomware-Angriffen betroffen sein.

Zusätzlich wird Druck auf die Opfer aufgebaut, indem mit der Veröffentlichung der erbeuteten Daten gedroht wird. Somit werden die verschlüsselten Daten selbst als weiteres Druckmittel eingesetzt.

Nach der Verschlüsselung der Daten, werden die Opfer zur Zahlung eines meist digitalen Lösegelds aufgefordert. Nach der Zahlung werden die Daten (vermeintlich) wieder freigegeben. Allerdings gibt es hierfür keine Garantie.[1]

Wie kann es zu einem Ransomware-Angriff kommen?

Bösartige E-Mail-Anhänge:
Angreifende versenden eine angeblich seriöse E-Mail, mit einer bekannten Institution als Absender. Im Anhang der E-Mail befindet sich eine Datei, die beim Öffnen die versteckte Schadsoftware automatisch herunterlädt.
Weitere Informationen hierzu finden Sie im Factsheet „Phishing-E-Mails“.

Bösartige Links in E-Mails:
Vermeintlich seriöse E-Mails können im Text Links enthalten, die beim Anklicken Schadsoftware herunterladen.

Drive-by-Downloads mittels Exploit-Kits:
Sogenannte Exploit-Kits sind Programmcode, der Schwachstellen in einem System ausnutzt. Nutzende werden dabei beispielsweise durch Werbung auf eine schädliche Website (um)geleitet. Schwachstellen im System ermöglichen das unbeabsichtigte Herunterladen von Schadsoftware (Drive-by-Download). Angreifende erhalten so Zugriff auf das System und können bösartige Software auf dem Gerät installieren.

Kompromittierte Zugangsdaten:
Cyberkriminelle nutzen erbeutete Zugangsdaten, um bösartige Software auf dem Gerät zu installieren**.**

Welche Schutzmaßnahmen gibt es? [1]

Updates:
Führen Sie regelmäßig und zeitnah zur Verfügung stehende Updates für Geräte und Programme durch.

Öffnen von Dateien/E-Mails:
Öffnen Sie -Dateien und E-Mails nur aus vertrauenswürdigen und Ihnen bekannten Quellen. Achten Sie bei Dateianhängen auf die Dateiendung (z. B. .pdf).
Weitere Informationen finden Sie im Factsheet „Phishing-E-Mails“.

Externe Speichermedien:
Schließen Sie niemals externe Speichermedien (z. B. USB-Sticks) aus unbekannter Quelle an Ihren Geräten an.

Backups/Datensicherung:
Sichern Sie Ihre Daten regelmäßig auf einem externen Speichermedium, das weder mit dem Internet noch mit dem Rechner dauerhaft verbunden ist.

Virenschutz:
Virenschutz-Programme können Schadsoftware erkennen.

E-Mail-Darstellung:
Um die Absenderadressen und Links richtig darzustellen, können Sie sich die E-Mail im „Nur-Text-Format“ anzeigen lassen.

Warum sollte kein Lösegeld bezahlt werden?

1. Es gibt keine Garantie, dass die Daten nach der Zahlung des Lösegelds tatsächlich wieder entschlüsselt werden.
2. Angreifende veröffentlichen in einigen Fällen trotz Zahlung des Lösegelds die Daten.
3. Die Informationen über die Zahlungsbereitschaft werden unter Angreifenden-Gruppierungen ausgetauscht. Das birgt die Gefahr, dass Sie erneut Opfer einer Erpressung durch Ransomware werden.

Quellen:

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html

Für weitere CSBW-Factsheets QR-Code scannen:

www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 08.2024
Kontakt: schulungen@cybersicherheit.bwl.de