RheinlandPfalz
LANDESKRIMINALAMT

HANDLUNGSEMPFEHLUNG RANSOMWARE

Mainz, 15.05.2017

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben.[1]

Täterseits werden Textdokumente erzeugt, aus denen entnommen werden kann, wie der Geschädigte vorgehen muss, um einen individuellen Decryptierungsschlüssel zu erwerben. Häufig erscheint auf dem Bildschirm ein Pop-up-Fenster mit der Nachricht, dass der Rechner erst nach Zahlung einer virtuellen Währung (z.B. Bitcoins) an die Cyberkriminellen wieder freigeschaltet wird.

Die Schadprogramme (Malware) gelangen beispielsweise über präparierte E-Mail-Anhänge, Links oder Drive-by-Exploits[2] über mit Schadsoftware infizierte Webseiten auf den Rechner.

Die aktuell durch die Erpresser weltweit eingesetzte Malware „WannaCry“ kann sich im Gegensatz zu älteren Ransomware-Arten eigenständig im betroffenen Netzwerk verteilen und breitet sich sehr schnell aus. Sowohl Wirtschaftsunternehmen als auch Privatpersonen können in unterschiedlichem Ausmaß durch diese Ransomware-Variante geschädigt sein oder werden.

---

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI)

[2] Beim Besuch auf präparierten Webseiten werden auf unzureichend geschützten Rechnern Schadprogramme auf dem System des Webseitenbesuchers installiert, ohne dass dieser etwas davon bemerkt. Betroffen sind sowohl dubiose als auch legitime Webseiten.

Wie die aktuelle Schadsoftware WannaCry die Systeme befällt kann zum gegenwärtigen Zeitpunkt nicht sicher gesagt werden.

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist aktuell keine Möglichkeit bekannt, die verschlüsselten Daten selbstständig, ohne Kontakt mit den Erpressern zu entschlüsseln.

Mit den nachfolgenden Handlungsempfehlungen möchte das Landeskriminalamt Rheinland-Pfalz Wirtschaftsunternehmen und anderen öffentlichen und nichtöffentlichen Institutionen sowie betroffenen Privatpersonen verschiedene Ansätze aufzeigen, mit denen sich eine wirkungsvolle Strategie gegen Malware erstellen lässt.

Die Realisierbarkeit der einzelnen Maßnahmen sowie deren Kombination bedürfen jeweils einer konkreten Einzelfallbetrachtung im Hinblick auf die vorhandene Unternehmensstruktur sowie auf das jeweilige Geschäftsmodell.

Handlungsempfehlungen:

- Machen Sie sich mit möglichen Bedrohungsszenarien vertraut
- Setzen Sie den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[3] als Grundlage eines professionellen Sicherheitskonzeptes um
- Identifizieren Sie regelmäßig den Schutzbedarf von Daten und Systemen
- Investieren Sie in die IT-Sicherheit Ihres Unternehmens
- Nutzen Sie ein vielschichtiges Verteidigungssystem (bspw. bestehend aus Firewalls, Intrusion Detection Systemen, Antispam-Software sowie Antivirenprogrammen) zur Verhinderung der Verbreitung der Schadsoftware
- Führen Sie regelmäßig Updates für die eingesetzten Softwareprodukte und Betriebssysteme durch
- Deinstallieren Sie nicht mehr benötigte Software
- Nutzen Sie die Möglichkeit einer Server- und Desktop-Virtualisierung um die betroffenen Systeme schnell neu auf- oder zurücksetzen zu können

[3] BSI: IT-Grundschutz; Link https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

- Speichern Sie besonders sensible Geschäftsdaten gegebenenfalls in einem isolierten Netzwerk
- Beobachten Sie regelmäßig die internen Netzwerke und kontrollieren Sie die Gateways zwischen den Netzwerksegmenten
- Stellen Sie Ihren E-Mail-Server so ein, dass die Annahme externer Mails mit internem Absender verhindert wird
- Überprüfen Sie alle E-Mails auf die richtige Absenderadresse sowie die korrekte Schreibweise der E-Mail Domain
- Seien Sie bei Eingang von E-Mails von unbekannten Absendern mit Anhängen oder LINKS besonders achtsam - es könnte sich um Schadcode handeln
- Verwenden Sie Office-Viewer zum Anschauen und Lesen verdächtiger Office-Dateien
- Deaktivieren Sie - sofern möglich - die Ausführung von Skripten in Betriebssystemen
- Verschlüsseln Sie Ihre Daten und nutzen Sie, sofern möglich, verschlüsselte Übertragungswege
- Verwenden Sie Verschlüsselungsmechanismen (z.B. Verschlüsselung von Datenträgern) und signieren Sie die E-Mails digital im Rahmen der internen und externen E-Mail-Kommunikation[4]
- Führen Sie regelmäßig Backups zur Datensicherung durch und überprüfen Sie die Wiederherstellbarkeit der Daten
- Legen Sie wichtige Daten immer auf Netzlaufwerken ab, da lokale Dateien unter Umständen nicht vom Backup erfasst werden
- Bewahren Sie die jeweils durchgeführten Backups noch einige Zeit auf, bevor diese wieder überschrieben werden
- Schränken Sie die Zugriffsberechtigungen auf das Nötigste ein. Über Administratorenrechte sollten nur ganz wenige ausgewählte Personen verfügen. Vergeben Sie, sofern möglich, für einzelne Benutzer lediglich Leserechte. Auch ein restriktiver Umgang mit Leserechten kann zum Schutz Ihrer Daten beitragen
- Führen Sie Zugriffsprotokollierungen durch

[4] BSI: Wie verschlüsselt kommunizieren?
www.bsi-fuer-buerger.de [...] Verschluesselung

- Verwenden Sie sichere (starke) Passwörter und ändern Sie diese in regelmäßigen Abständen. Eine besondere höhere Sicherheit bieten bspw. Zwei-Faktor-Authentifizierungen[5]
- Führen Sie Awareness-Kampagnen durch
- Ergreifen Sie Maßnahmen zur Sensibilisierung und Schulung der Mitarbeiter/-innen
- Definieren Sie Anforderungen an Geschäftspartner oder Dienstleister
- Erstellen Sie IT-Sicherheitskonzepte, Sicherheitsrichtlinien und Notfallpläne und flankieren Sie diese durch firmeninternes Controlling
- Tauschen Sie sich regelmäßig mit anderen Unternehmen und Behörden zu aktuellen Bedrohungen aus

Sollten Sie, Ihr Unternehmen oder Ihre Behörden bereits Opfer einer Ransomware-Erpressung sein, rät das Landeskriminalamt Rheinland-Pfalz dringend davon ab, der Lösegeldaufforderung nachzukommen!

<u>Maßnahmen nach einer Infektion</u>

- Trennen Sie unverzüglich die Netzwerkverbindung von infizierten Rechnern
- Schalten Sie betroffene Geräte umgehend aus, um eine weitere Verschlüsselung der Daten zu verhindern
- Isolieren Sie - sofern möglich - relevante Dateien, die Aufschluss über den Infektionshergang geben können (z.B. Log-Dateien oder E-Mails)
- Speichern Sie verschlüsselte Daten, die nicht über ein Backup rekonstruiert werden konnten, gesondert. Möglicherweise wird durch die Anti-Viren-Industrie bzw. das BSI in Zukunft eine Schwachstelle gefunden werden, über die letztlich eine Rekonstruktion dieser Daten möglich ist (Entschlüsselungstool). Hierzu sollte zusätzlich eine der decrypt-Text Anweisungen gesichert werden
- Ändern Sie vorsorglich Ihre Benutzer- und Netzwerkkennwörter

[5] BSI: Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. *https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/glossar_node.html*

Sofern Ihr Unternehmen oder Ihre Behörde bereits Ziel eines Cyberangriffs geworden sein sollte, können Sie sich an die örtliche Polizeidienststelle oder an die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Rheinland-Pfalz wenden.

Privatpersonen werden gebeten, Strafanzeige bei der jeweils örtlich zuständigen Polizeidienststelle zu erstatten.

Herausgeber
Landeskriminalamt Rheinland-Pfalz
Valenciaplatz 1-7
55118 Mainz
E-Mail: lka.@polizei.rlp.de
Internet: www.polizei.rlp.de