Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im August 2014

Sehr geehrte Damen und Herren,

betriebliche Daten, welche auf IT-Systemen gespeichert werden, sind einer immer größeren Bedrohung durch eine Vielzahl von Angreifern ausgesetzt.

Aus gegebenem Anlass möchten wir Ihnen Informationen zum Themenfeld Schutz von digitalen Daten anbieten, da dem niedersächsischen Wirtschaftsschutz von der Zentralen Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Niedersachsen steigende Angriffszahlen auf die Integrität von gespeicherten Daten gemeldet werden.

Es zeigt sich hier, wie wichtig es ist, auch im Bereich des Datenbackups eine stringente Sicherheitsstrategie zu fahren.

Für Rückfragen zu diesem Thema stehen wir jederzeit gerne zur Verfügung, wobei das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen unberührt bleibt.

Ihr Wirtschaftsschutz-Team

Niedersächsische Verfassungsschutzbehörde

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

Falldarstellung

Meldungen des ZAC über die Ransomware[1] Cryptolocker zeugen von einer steigenden Verbreitung dieser Art von Schadsoftware. Die Schadsoftware scheint sich über infizierte E-Mail Anhänge und über präparierte Webseiten, so genannte Drive-By-Downloads, zu verbreiten. Nach Installation, verschlüsselt die Schadsoftware die Dateien, welche sich auf dem Computer des Anwenders befinden (beispielsweise Excel- oder Word-Dateien).
Eine neue Variante Namens Synolocker greift ausschließlich ältere Synology NAS-Geräte an und verschlüsselt die auf dem NAS[2] gespeicherten Daten.
Verschiedene Antiviren Produkte können die Schadsoftware entdecken und löschen, dann ist es aber meistens zu spät, weil die auf dem Computer vorhandenen Dateien bereits verschlüsselt wurden. In diesem Fall ist deshalb nicht die Entfernung der Schadsoftware das Problem, sondern die Wiederherstellung der ursprünglichen Daten.

Wie können Sie sich schützen:

- Auf dem Computer abgelegte Daten sollten regelmäßig auf externe Datenträger kopiert werden (Backup). Diese sollten **nur** während des Backupvorgangs am Computer angeschlossen sein.
- Sowohl Betriebssystem als auch installierte Applikationen (z.B. Adobe Reader, Adobe Flash, Sun Java etc.) müssen immer auf den neuesten Stand gebracht werden. Falls vorhanden, am besten mit der automatischen Update Funktion.
- Ein Antivirenprogramm muss installiert und auf dem neuesten Stand sein.
- Eine Personal Firewall muss installiert und auf dem neusten Stand sein.
- Seien Sie immer vorsichtig bei verdächtigen E-Mails, bei E-Mails, welche Sie unerwartet bekommen, oder welche von einem unbekannten Absender

[1] Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt, welche aufgehoben werden soll durch Zahlung von "Lösegeld".
[2] Network Attached Storage (NAS, englisch für netzgebundener Speicherplatz) bezeichnet einfach zu verwaltende Dateiserver.

stammen. Befolgen Sie hier keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links.

Sollten Sie bereits Opfer von Cryptolocker sein:

Es ist ein Entschlüsselungs-Tool für Opfer von CryptoLocker verfügbar.
Die IT-Sicherheitsdienstleister FireEye und Fox-IT haben einen Gratis Service zur Verfügung gestellt, der es Opfern von Cryptolocker ermöglicht, die durch die Schadsoftware verschlüsselten Daten wieder zurückzuerlangen. Wie in den Medien berichtet, hat das FBI bereits Anfangs Juni gegen das Cryptolocker Botnetzwerk Maßnahmen ergriffen, doch es gibt noch zahlreiche Benutzer, deren Daten verschlüsselt sind.

Der Service ist unter der Adresse https://www.decryptcryptolocker.com verfügbar. Für die Nutzung dieses Dienstes ist weder eine Bezahlung noch eine Anmeldung notwendig.

Die Vorgehensweise ist nachfolgend beschrieben:

- Zuerst wird eine verschlüsselte Datei von Ihrem Computer benötigt. Achten Sie darauf, dass diese keine sensiblen Informationen enthält.
- Diese Datei laden Sie auf die Plattform https://www.decryptcryptolocker.com hoch. Außerdem ist eine E-Mail Adresse anzugeben, an welche die Resultate gesendet werden sollen.
- Sie erhalten danach eine E-Mail mit einem Schlüssel und einem Download-Link, um das Entschlüsselungs-Programm herunterzuladen, mit welchem Sie die Dateien entschlüsseln können.
- Starten Sie dieses Programm lokal auf ihrem Computer und geben Sie den Schlüssel ein.
- Die auf dem Computer vorhandenen verschlüsselten Dateien werden nun durch das Entschlüsselungs-Programm entschlüsselt.

Auch im Falle von Synolocker ist es nicht ausgeschlossen, dass durch Recherchen und Ermittlungen, die entsprechenden Kryptoschlüssel, wie im Fall von Cryptolocker, zu einem späteren Zeitpunkt sichergestellt werden können. Aus diesem Grund sollten durch Synolocker verschlüsselte Daten auf jeden Fall aufbewahrt werden.

Quellen:

ZAC (Zentrale Ansprechstelle Cybercrime, LKA Niedersachsen)
MELANI (Schweizer Melde- und Analysestelle Informationssicherung)

Ein interessanter Link in anderer Sache:

Die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. Andre Hahn, Ulla Jelpke, weitere Abgeordneter und der Fraktion DIE LINKE zu geheimdienstlichen Angriffen und Spionage bei deutschen Unternehmen finden sie unter:

http://dipbt.bundestag.de/dip21/btd/18/022/1802281.pdf