POLIZEIDIREKTION
HANNOVER

Polizeidirektion Hannover, Waterloostr. 9, 30169 Hannover

Polizeidirektion Hannover
Presse- und Öffentlichkeitsarbeit

Presseinformation

Ryuk – so funktioniert die Erpressungssoftware

Bei dem Programm „Ryuk“ handelt es sich um sogenannte Ransomware (Englisch ransom = Lösegeld, ware = Abkürzung für Software). Gelangt das Programm auf einen Computer oder ein Netzwerk, fährt es mehrere Hundert Prozesse und Dienste des Systems herunter, die es daran hindern können, die folgenden Schritte auszuführen. Als Nächstes verschlüsselt das Programm Dateien, die sensible Daten und Informationen enthalten könnten wie Fotos, Videos, Dokumente oder auch ganze Datenbanken. Gelingt der Ransomware das Eindringen in einen PC oder ein Netzwerk, wird auf dem Endgerät eine Text-Datei mit einer Lösegeldforderung hinterlassen. In dem Text wird darüber hinaus beschrieben, dass eventuelle Systemkopien (z. B. Backups) ebenfalls verschlüsselt oder sogar gelöscht wurden. Die Schadsoftware zu entfernen oder das System auf einen Zeitpunkt vor dem Angriff zurückzusetzen, führt dazu, dass auch im Fall einer Zahlung die Dateien nicht wieder entschlüsselt werden könnten. Eine manuelle Entschlüsselung, ohne den Schlüssel von den Tätern zu erwerben, ist bei dem jetzigen Stand der Technik ausgeschlossen. Das Lösegeld muss also zum Erhalt des Systems gezahlt werden. Dringt die Schadsoftware in ein Netzwerk von Computern ein, ist sie in der Lage, auch ausgeschaltete Rechner des Netzwerkes einzuschalten (z. B. über eine WLAN-Verbindung), auch diese zu infizieren.

Das Befallen der Netzwerke und PCs erfolgt meist über eine sogenannte Phishing-Mail - eine E-Mail mit einem Link oder einer Datei im Anhang. Öffnet man Link oder Datei, installiert sich Ransomware, die „Ryuk“ nachlädt und somit als „Türöffner“ dient. Das dann infizierte Endgerät wird durch die Täter als Einfallstor zu großen Netzwerken genutzt, um diese auszuspähen und die Ransomware auf alle anderen Geräte des Netzes auszurollen. Die Phishing-Mails sind bewusst so formuliert, dass die Adressaten annehmen, dass es sich um eine rechtmäßige Nachricht handelt und das Öffnen des
Anhangs stelle keine Gefahr darstellt.

Ziel der Angriffe von „Ryuk“ sind meist Firmen, Behörden und Institutionen, deren Funktion an eine schnelle Infrastruktur gebunden ist und/oder die sensible Kundendaten verwalten. Also Einrichtungen, bei denen ein Befall der Schadsoftware großen Schaden zum Nachteil vieler Tausend Personen und in Millionenhöhe anrichten kann und die Erpresser somit die Zeit als Druckmittel haben. So werden zum Beispiel Krankenhäuser mit der Ransomware „Ryuk“ angegriffen. „Ryuk“ wird auch als sogenanntes RaaS-Programm (RaaS = Ransomware as a Service) angeboten. Eine kriminelle Gruppierung bietet es einer anderen an und wird prozentual an der erpressten Beute beteiligt.

Polizeidirektion Hannover
Waterloostr. 9
30169 Hannover
Paketanschrift
Hardenbergstr. 1
30169 Hannover

Telefon
0511 109-1041 bis -1046
Telefax
0511 109-1040
Web
www.polizei-hannover.de

E-Mail, Website
pressestelle@pd-h.polizei.niedersachsen.de
Bankverbindung Nord/LB
IBAN: DE73 2505 0000 0106 0209 44
SWIFT-BIC: NOLADE2H
USt-IDNr.: DE174239046