Uniklinik Düsseldorf: Ransomware "DoppelPaymer" soll hinter dem Angriff stecken

heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html

Olivia von Westernhagen

Die Verantwortlichen für den Angriff auf die Uniklinik sitzen laut Justizministerium möglicherweise in Russland. Die Ermittlungen und Aufräumarbeiten dauern an.

Lesezeit: 4 Min.

(Bild: Shutterstock/BlurryMe)

22.09.2020 14:19 Uhr
Security

Von
Olivia von Westernhagen

Nach dem Angriff auf die Düsseldorfer Uni-Klinik führt eine mögliche Spur der Täter laut Justizministerium nach Russland. So hätten die Angreifer eine Schadsoftware namens "DoppelPaymer" in das System geschleust. Dieser Verschlüsselungstrojaner sei bereits in zahlreichen anderen Fällen weltweit gegen Unternehmen und Institutionen von einer kriminellen Hacker-Gruppe eingesetzt worden, die nach Einschätzung privater Sicherheitsunternehmen in der Russischen Föderation beheimatet sein soll. Das teilte das Ministerium von Nordrhein-Westfalen am Dienstag laut dpa in einem Bericht an den Rechtsausschuss mit.

Die Cybercrime-Bande hinter DoppelPaymer hat sich ähnlich wie die mit der Emotet-Gang zusammenarbeitende Trickbot-Bande auf das Erpressen von Firmen und Organisationen spezialisiert. Sie setzen ebenfalls sehr ausgefeilte Techniken ein, um sich in den Netzen auszubreiten und dabei unbemerkt zu bleiben, bis sie tatsächlich Daten verschlüsseln. Ihre Lösegeldforderungen richten sich nach dem "Wert" des jeweiligen Angriffsziels und können Millionenhöhe erreichen. Mitte März dieses Jahres hatte die DoppelPaymer-Gang, wie auch einige andere Ransomware-Gruppen, eine "Corona-Pause" für Krankenhäuser versprochen – ein Versprechen, das sie dann doch nicht einhielt.

Einbruch via "Shitrix" bestätigt

Die Ermittler wissen inzwischen, dass die kriminellen Hacker zunächst einen sogenannten "Loader" zum Nachladen des eigentlichen Schadprogramms ins System der Uni-Klinik einschmuggelten. Offen blieb in dem Bericht, wann das war. Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hatte vergangene Woche mitgeteilt, dass die entsprechende Sicherheitslücke in Software von Citrix bereits seit dem Jahreswechsel bekannt war. Dabei handelte es sich um eine Lücke in der Citrix-VPN-Software, die unter dem Namen "Shitrix" bekannt wurde (CVE-2019-19781):

Lesen Sie auch

Cyber-Angriff auf Uniklinik Düsseldorf: #Shitrix schlug zu

Die Uni-Klinik hatte nach eigenen Angaben damals sofort reagiert. Zwei Spezialfirmen hätten das System noch einmal überprüft – ohne Hinweis auf eine Gefährdung durch die nun geschlossene Sicherheitslücke. Offenbar schlummerte der "Loader" da aber bereits auf einem Server der Uni-Klinik.

Das wahrscheinlichste Szenario ist somit derzeit, dass die Cyberkriminellen die Shitrix-Lücke sehr bald nach ihrem Bekanntwerden und noch vor der Bereitstellung des Patches durch Citrix ausgenutzt haben. Sie sind dann darüber in das Netz der Uni-Klinik eingedrungen und haben dort heimlich eine Backdoor platziert. Das kann durchaus auch auf einem anderen System als dem eigentlichen VPN-Server geschehen sein, sodass die Hintertür beim Installieren der Citrix-Updates nicht gefunden wurde. Erst jetzt, viele Monate später, haben sie diese Backdoor benutzt, um wieder Zugriff auf das Netz der Uni-Klinik zu erlangen.

Täter halfen nach "Irrtum" beim Entschlüsseln

Der eigentliche Angriff durch die nachgeladene Verschlüsselungssoftware passierte erst in der Nacht vom 10. auf den 11. September. 30 Server der Uni-Klinik wurden durch das Schadprogramm verschlüsselt – wobei die Cyberkriminellen eigentlich wohl die Düsseldorfer Universität attackieren wollten. Zu der hatten sie ein digitales Erpresserschreiben adressiert. Als die Polizei den Tätern ihren mutmaßlichen Fehler mitteilte, schickten diese einen digitalen Schlüssel, um das Krankenhaus wieder zum Laufen zu bekommen.

Die Ermittler vermuten laut dem Bericht an den Landtag, dass die Uni-Klinik Opfer einer "weltweiten kommerziellen Malware-Kampagne" geworden sein könnte. Weitere Details nannte ein Sprecher der zuständigen Staatsanwaltschaft bei der Zentrale- und Ansprechstelle Cybercrime (ZAC) am Dienstag nicht. Laut einer Statistik der US-amerikanischen Temple University liegt die Frequenz der Attacken mit Erpresser-Software dieses Jahr auf dem Höchststand seit 2013. Dabei gezählt wurden allerdings nur die öffentlich bekannten Angriffe. Ermittler gehen von einer hohen Dunkelziffer aus, bei der zum Beispiel Unternehmen auf die Forderungen der Erpresser eingehen.

Ermittlungen und Bereinigung laufen weiter

Die Ermittlungen um den Verdacht der fahrlässigen Tötung einer Patientin liefen unterdessen weiter, erklärte der ZAC-Sprecher. Die Frau war statt in die nahe Uni-Klinik in ein weiter entferntes Krankenhaus nach Wuppertal gebracht worden und gestorben. Für den Vorwurf der fahrlässigen Tötung könnte unter anderem entscheidend sein, ob die Frau eine Überlebenschance gehabt hatte, wenn sie in die Uni-Klinik gekommen wäre.

Die IT des Krankenhauses ist unterdessen weiter nicht voll einsatzbereit. Die größte Klinik der Landeshauptstadt rechnet nach Angaben eines Sprechers damit, dass die Zentrale Notaufnahme diese Woche eventuell ihren Dienst wieder aufnehmen kann. Noch seien aber nicht alle entsprechenden Systeme wieder hochgefahren.

Lesen Sie auch

Cybercrime: Erpressung auf neuem Niveau

(ovw)