2021/22 Networld

https://shop.jungle.world/artikel/2021/22/game-over

Hacker legten ein Pipelinesystem in den USA lahm, um Geld zu erpressen

Game Over

Von **Enno Park**

Ein Hackerangriff auf ein Pipeline-System schränkte für einige Tage die Benzinversorgung in den USA ein. Diese Art technischer Erpressung ist eine hochprofitable Form der organisierten Kriminalität.

Mitte Mai ging in Teilen der USA der Sprit aus. 87 Prozent der Tankstellen in Washington, D.C., saßen auf dem Trockenen, Autobesitzer kauften panikartig Benzin, die Fluggesellschaft American Airlines musste Flugpläne wegen Treibstoffmangels ändern. Der Benzinpreis stieg auf den höchsten Stand seit 2014, umgerechnet knapp 66 Eurocent pro Liter.

Das Problem war allerdings nicht ein Mangel an Benzin, sondern dass dieses nicht mehr transportiert werden konnte: Die Rechnerinfrastruktur des Betreibers Colonial Pipeline, dessen Pipeline-System über Tausende Kilometer Benzin, Heizöl und andere Ölprodukte vom Bundesstaat Texas aus an die Ostküste der USA liefert und dort verteilt, war gehackt worden.

> Die Hackergruppe Darkside versprach, dafür zu sorgen, dass ihre Kunden ihre Opfer sorgfältiger aussuchen, »um in Zukunft gesellschaftliche Auswirkungen zu vermeiden«.

Die Computer der Betreiberfirma waren mit Ransomware, also Erpressungssoftware infiziert worden. Hat diese einen Computer befallen, verschlüsselt sie alle Daten auf der Festplatte. Der Nutzer wird dann aufgefordert, eine Geldsumme zu überweisen, um die Festplatte wieder entschlüsseln zu können. In der Regel funktioniert das auch, was nicht so sehr an der Ganovenehre der Hacker liegt als eher daran, dass die Masche langfristig nur funktionieren kann, wenn die Erpressten auch erwarten können, dass sie eine Gegenleistung bekommen, wenn sie bezahlen.

So war es auch in diesem Fall: Wie Verantwortliche von Colonial Pipeline US-Medien mitteilten, zahlte das Unternehmen 75 Bitcoin, umgerechnet rund 4,4 Millionen US-Dollar, an die Erpresser und erhielt daraufhin die Software zum Entschlüsseln der Daten. Das

Rettungsprogramm stellte sich jedoch als so langsam heraus, dass es schneller ging, die Systeme aus vorhandenen Backups wiederherzustellen. Sechs Tage nach Beginn des Angriffs wurde das Pipeline-System schrittweise wieder in Betrieb genommen.

Technisch kann so ein Angriff auf unterschiedlichen Wegen erfolgen. Der vermutlich häufigste Verbreitungsweg ist ein E-Mail-Anhang, den das Opfer arglos anklickt. Solche Mails werden häufig wahllos an viele Adressen geschickt, oft werden aber auch individuell zugeschnittene, möglichst glaubwürdige E-Mails an bestimmte Individuen versendet, um gezielt ein Unternehmen anzugreifen. Die Software kann auch über kontaminierte USB-Sticks eingeschmuggelt werden, oder die Hacker suchen die Router, mit denen die Firmenrechner mit dem Internet verbunden sind, nach Sicherheitslücken ab; der Wurm Wannacry 2017 hingegen nutzte Sicherheitslücken des Betriebssystems Windows aus.

Die Erpressung des Pipeline-Betreibers ist kein Einzelfall. Längst handelt es sich um eine eigene Branche organisierter Kriminalität. Einem Bericht des IT-Sicherheitsdienstleister Coveware zufolge richten Ransomware-Attacken immer mehr Schaden an, voriges Jahr waren es 20 Milliarden US-Dollar. Den Angreifer von Colonial Pipeline, nach Angaben des FBI eine russische Hackergruppe namens Darkside, muss man sich wie ein professionelles IT-Unternehmen vorstellen. Selbst der Kundendienst soll höchsten Standards genügen. Wie frühere Fälle zeigen, werden die Erpressten umfassend und durchaus freundlich von Darkside-Mitarbeitern unterstützt, die per Chat Fragen beantworten sowie durch den Bezahl- und Entschlüsselungsprozess lotsen. Mit Darkside-Software werden die betreffenden Unternehmen nicht nur erpresst, indem diese die Computersysteme lahmlegt, sondern sie wird häufig auch verwandt, um Daten zu stehlen und mit der Drohung, diese zu veröffentlichen, Geld zu erpressen.

Nicht nur für die Erpressten, sondern auch für andere Kriminelle fungiert Darkside wie ein Serviceunternehmen. Die Gruppe bietet ihren Kunden die spezielle Dienstleistung der Verschlüsselung und des Zahlungsempfangs. Gelingt dem Kunden auf diese Weise der Coup, bekommt Darkside eine Provision, zehn bis 25 Prozent der erpressten Summe.

Der Sitz von Darkside wird in Russland vermutet. Auch über einen russischen Angriff auf die US-Infrastruktur war deshalb spekuliert worden, als an der Ostküste der Sprit knapp wurde. Doch dass es sich um eine Cyberattacke des russischen Staats handelte, ist eher unwahrscheinlich; die US-Regierung geht nicht davon aus. Der Angriff entspricht nicht dem Muster bisheriger wahrscheinlich Russland zuzuschreibender Attacken, zum Beispiel des Angriffs auf die texanische IT-Firma Solarwinds Ende vorigen Jahres (*Jungle World* 1/2021) oder desjenigen auf den deutschen Bundestag 2015. Diese Cyberangriffe dienten der Spionage, es wurden Daten erbeutet. Staatliche Cyberattacken mit dem Ziel, in einem anderen Land materiellen Schaden anzurichten, sind sehr selten, denn sie sind extrem aufwendig gemessen an dem ungewissen strategisch-politischen Nutzen, besonders wenn sie ein bestimmtes Ziel treffen sollen.

Weil bei den meisten Hacks die Schäden nicht gut kalkulierbar sind, fügen sich Cyberangriffe nicht recht in die gängigen Eskalations- und Deeskalationsmuster zwischenstaatlicher Konflikte ein. Staaten wissen oft nicht, wie sie auf Cyberangriffe reagieren sollen, und auch nicht, wie ihr Gegenüber reagieren wird, wenn sie selbst einen

Cyberangriff unternehmen. Deshalb gibt es nur wenige Beispiele von Cyberkriegsführung, zum Beispiel den wahrscheinlich US-amerikanischen Angriff auf iranische Atomanlagen mit dem Schadprogramm Stuxnet 2010. Spionageangriffe wie der Hack des Bundestags oder auch der Nordkorea zugeschriebene Angriff auf Sony Pictures aus Rache für die Veralberung des Diktators Kim Jong-un in dem Film »The Interview« 2014 werden bislang als nicht schwerwiegend genug angesehen, um nennenswerte Konsequenzen nach sich zu ziehen.

Erpressung mit Verschlüsselungssoftware ist bei solchen staatlichen Attacken erst recht nicht im Spiel, weil die Angreifer nicht erkannt werden wollen. Bei Spionagehacks soll am besten niemand merken, dass überhaupt ein Angriff stattgefunden hat. Es ist zwar denkbar, dass ausländische Mächte eine Ransomware-Attacke zur Tarnung eines Angriffes auf die Infrastruktur in anderen Ländern verwenden, doch zumindest beim Fall von Colonial Pipeline sind keine Hinweise bekannt, die darauf hindeuten.

Dennoch schienen der Hackergruppe die Auswirkungen ihres Angriffs auf das US-Pipeline-Netzwerk und die mögliche Reaktion der US-Regierung Sorgen zu bereiten. »Wir sind unpolitisch, wir haben mit Geopolitik nichts zu tun, uns muss man nicht mit einer bestimmten Regierung in Verbindung bringen«, hieß es Anfang Mai auf einem offenbar von der Hackergruppe betriebenen Blog. »Unser Ziel ist es nur, Geld zu verdienen.« Die Hacker versprachen, dafür zu sorgen, dass ihre Kunden ihre Opfer sorgfältiger aussuchen, »um in Zukunft gesellschaftliche Auswirkungen zu vermeiden«. Die Gruppe legte in der Vergangenheit eine gewisse Robin-Hood-Attitüde an den Tag, wenn sie versuchte, einen kleinen Teil ihrer Einnahmen an gemeinnützige und wohltätige Organisationen zu spenden, die sich allerdings dagegen verwahrten.

Die steigende Zahl von Ransomware-Erpressungen in den vergangenen Jahren ist tatsächlich weniger die Folge von Machenschaften irgendwelcher Regierungen. Sie ist auch keine automatische Folge wachsender Digitalisierung, sondern vor allem auf das Aufkommen der Kryptowährung Bitcoin zurückzuführen. Schadsoftware, Angriffe auf Computersysteme und Cyberkriminalität gibt es bereits seit vielen Jahren, aber erst Bitcoin ermöglichte weitgehend anonyme, kaum nachverfolgbare digitale Geldübergaben. Auch die Online-Shops für illegale Güter im Darknet profitieren seit einem Jahrzehnt von Bitcoin und andere Kryptowährungen.

Doch auch wenn die russische Regierung wahrscheinlich nicht involviert ist, trägt sie eine gewisse Mitverantwortung für den Angriff auf Colonial Pipeline. Russland ist seit Jahren eine Art Freibeuterhafen für Cyberkriminelle. Die russischen Gesetze sind diesbezüglich sehr streng, finden aber nur Anwendung, wenn Russen Opfer der Angriffe sind. Attacken auf ausländische Ziele werden stillschweigend geduldet, was auf eine Art Übereinkunft hinausläuft: Die Erpressungssoftware fragt die Spracheinstellungen des Computersystems ab. Verwendet dieses Russisch oder eine andere im postsowjetischen Raum gängige Sprache, stellt sie oft ihre Arbeit ein. Unter Umständen kann man sogar den Schlüssel von den Erpressern erhalten, ohne dafür zu zahlen, wenn man ihnen mit einem Ausweisdokument glaubhaft machen kann, dass man Russe ist. Von einem solchen Fall berichtete unter anderem der IT-Sicherheitsexperte Linus Neumann im Podcast »Logbuch Netzpolitik«.

Wie und ob es mit Darkside weitergeht, ist indes ungewiss. Vielleicht waren die Hacker erschrocken, welche Auswirkungen ihr Angriff auf die Pipeline hatte; vielleicht fürchten sie nun doch, die Duldung russischer Behörden zu verlieren, oder haben aufgrund der Größe des Schadens kalte Füße bekommen. Jedenfalls besagt die letzte Mitteilung auf ihrer Website, dass sich die Gruppe aufgelöst habe. Experten bezweifeln das allerdings.