Ransomware: technische, nationale und multilaterale Gegenmaßnahmen

Schulze, Matthias

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Schulze, M. (2021). *Ransomware: technische, nationale und multilaterale Gegenmaßnahmen.* (SWP-Aktuell, 56/2021). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2021A56

SWP

SWP-Aktuell

NR. 56 AUGUST 2021

Ransomware

Technische, nationale und multilaterale Gegenmaßnahmen

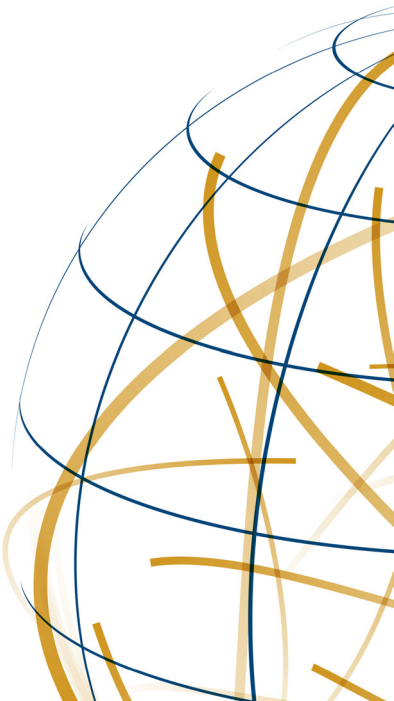
Matthias Schulze

Während Ransomware-Angriffe immer professioneller werden, haben viele Organisationen grundlegende IT-Sicherheitshausaufgaben noch immer nicht gemacht. Aufgrund der effektiven Untergrundökonomie der Cyber-Kriminellen ist dem Problem auch nicht mehr allein mit technischen Maßnahmen beizukommen. Die neue Bundesregierung sollte es mit erhöhter Priorität und einer gesamtstaatlichen Perspektive angehen. Neben Präventionsmaßnahmen sollten auch für Organisationen in der Breite Pläne zur Reaktion und Wiederherstellung erstellt werden. Außerdem ließen sich Instrumente nutzen, die etwa bei der Bekämpfung von organisierter Kriminalität, Terrorismus oder Finanzkriminalität und sogar in der Entwicklungshilfe eingesetzt werden. Schließlich müssten multilaterale Initiativen zur Eindämmung von Cyber-Kriminalität und Geldwäsche mit Kryptowährungen gestärkt werden.

Ransomware ist eine Form von Schadsoftware, die ein betroffenes System verschlüsselt und bewirkt, dass sich Daten nicht mehr verwenden lassen. Kriminelle versprechen gegen die Zahlung eines Lösegelds in Kryptowährungen die Freigabe der Daten. Für viele Organisationen bedeutet ein Verlust der Datenverfügbarkeit oft das unfreiwillige Ende des operativen Betriebs und verursacht somit hohe wirtschaftliche Kosten. Der »State of Ransomware 2021«-Bericht der Firma Sophos zeigt, dass die Hälfte von 5.400 weltweit befragten Unternehmen bereits betroffen war. Laut einer Befragung von 200 Firmen durch die International Data Corporation (IDC) wurden schon 78 % der deutschen Unternehmen erfolgreich attackiert. IT-Experten warnen daher, dass es nur eine Frage der Zeit sei, wann eine Organisation betroffen sein wird. Zwar gibt es Ransomware schon seit den 1980er Jahren, doch haben eine Reihe von Dynamiken dazu geführt, dass sich das Problem heute in Qualität und Quantität dramatisch verschärft hat.

Problemlage und aktuelle Dynamiken

Die Corona-Pandemie und die Verlagerung ins Home-Office haben weltweit IT-Systeme verwundbarer gemacht. Organisationen haben hastig mobiles Arbeiten ermöglicht und ihre sensiblen internen Netzwerke für ihre daheim tätigen Mitarbeiterinnen und Mitarbeiter geöffnet. Dieser Fernzugriff auf Systeme, etwa zur Administration, ist heute



Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

neben Emails und Schwachstellen in Firmen-VPN ein vorherrschender Angriffsvektor. Die jüngste massive Umstrukturierung der IT wurde oft nicht mit zusätzlichen IT-Supportstellen und Schutzmaßnahmen begleitet. Die Folge ist ein massiver Anstieg der Ransomware-Fälle (um 485% gegenüber 2019 laut Bitdefender).

Während vor einigen Jahren undifferenzierte Angriffe gegen Opportunitätsziele mit geringem IT-Sicherheitsniveau dominierten, geht der Trend heute zum »big game hunting«. Kritische Infrastrukturen und größere Unternehmen wie Öl-Pipeline-Betreiber, Supermarktketten, aber auch IT-Unternehmen wie Acer werden systematisch angegriffen. Dazu werten Kriminelle Quartalsberichte aus und errechnen die zu fordernden Lösegelder, die bewusst geringer sind als die geschätzten Kosten zur Wiederherstellung der IT betroffener Unternehmen, um die Anreize für die Bezahlung zu erhöhen. Oft sind auch mittelständische Unternehmen betroffen, die umsatzstark, aber vielfach nicht kritisch genug sind, als dass Angreifer staatliche Konsequenzen zu befürchten hätten. Kleinere, kommunale kritische Infrastrukturen wie Wasserwerke sind besonders verwundbar, da ihnen nicht selten ein angemessenes IT-Sicherheitsbudget fehlt.

Waren vor einigen Jahren Zahlungen geringerer Lösegeldsummen ein verkraftbares Ärgernis für die meisten Unternehmen, sind Angreifer inzwischen skrupelloser geworden und verlangen Millionenbeträge — und erhalten sie auch. Die Gruppe REvil forderte von der IT-Firma Kaseya im Juni 2021 rekordverdächtige 70 Millionen Dollar Lösegeld. Durchschnittliche Lösegeldsummen liegen mittlerweile bei rund 300.000 US-Dollar. Dies kann kleinere Unternehmen in Existenznöte bringen, insbesondere wenn sich derlei Vorfälle binnen kurzer Zeit wiederholen. Für solche Unternehmen ist es schwieriger, die damit verbundenen Umsatzeinbußen zu verkraften und die Mittel für die Wiederherstellung von Infrastruktur aufzubringen. Die Umsatzeinbußen belaufen sich im Schnitt auf das Fünf- bis Zehnfache der Ransomzahlungen.

Angreifer sind zudem agiler und schneller geworden als die meist schwerfälligen Bürokratien und IT-Abteilungen, die oftmals Geld für neue Abwehrmaßnahmen langwierig einfordern müssen. Laut einer Studie von 2018 schützen traditionelle Antivirensysteme nicht mehr gegen die meisten Ransomware-Angriffe. Denn Ransomware-Gruppen lernen von ihrer Konkurrenz und auch von staatlichen Cyber-Angriffstechniken und verbessern so ihre eigenen Operationen. Zudem reinvestieren sie die erpressten Lösegeldsummen in immer neue und noch komplexere Angriffstechniken (oder subventionieren damit andere kriminelle Praktiken wie Drogenhandel). Nimmt man in einem hypothetischen Beispiel die Lösegeldgewinne der Angreifergruppe REvil von rund 40 Millionen US-Dollar als Bezugswert, die sich in neue Angriffswerkzeuge investieren lassen, würde diese Summe den IT-Haushalt der meisten mittleren und größeren Unternehmen übersteigen. Mit so hohen Beträgen können Angreifer traditionelle und häufig schnell veraltete Schutzmaßnahmen der Verteidiger, die über ein weitaus geringeres IT-Sicherheitsbudget verfügen, problemlos ausmanövrieren. Ein Beispiel sind »supply chain«-Angriffe. Diese richten sich gegen Dienstleister, die ihren Klienten etwa Netzwerk- oder Software-Management bieten. Diese Form von Angriffen wurde vor wenigen Jahren noch weitgehend exklusiv von staatlichen Nachrichtendiensten genutzt, wird aber zunehmend auch von Kriminellen nachgeahmt.

Ein weiteres Indiz für die fortschreitende Professionalisierung ist die Ausnutzung komplexerer Sicherheitslücken. Während Ransomware in den vergangenen Jahren vorwiegend bei bekannten, von Betroffenen noch nicht per Update behobenen Sicherheitslücken ansetzte, kaufen Angreifer mittlerweile auch Informationen über sogenannte 0-Day-Sicherheitslücken auf Schwarzmärkten ein bzw. haben die Fähigkeit, diese selber zu entwickeln. Damit können sie auch Ziele angreifen, die durch ein hohes Maß an IT-Sicherheit geschützt sind, welche gegen 0-Days aber nichts aus-

zurichten vermag. Einige Kriminelle operieren mittlerweile auf einem ähnlichen Professionalitätsniveau wie einige Staaten. Halfen vor wenigen Jahren noch Backups halbwegs zuverlässig gegen Ransomware, da dank vorhandener Datenkopie der Erpressungsversuch ins Leere ging, verschlüsseln moderne Angreifer heute nicht nur Daten, sondern stehlen sie auch und drohen mit Veröffentlichung (»double extortion«).

Marktfaktoren und Proliferation

Die Professionalisierung folgt einer marktorientierten Entwicklung. Ransomware als äußerst profitables Geschäftsmodell hat eine ganze Untergrundökonomie mit spezialisierten Dienstleistungen entstehen lassen. Schadsoftwareentwickler vermieten ihre Software an »affiliates«, die Gewinne werden geteilt. Spezialisierte Dienstleister bieten mietbare Botnetze zum automatisierten Verbreiten von Schadsoftware über Emails an. Gegen Strafverfolgung abgesicherte besondere Server (»bullet proof hosts«) werden als »Command & Control«-Infrastruktur zur Steuerung von Schadsoftware vermietet. Den Zugang zu bereits kompromittierten und damit weiter infizierbaren Rechnern verkaufen sogenannte »access broker«. Dank grafischer Benutzeroberflächen und automatisierter Prozesse lässt sich Ransomware zudem immer einfacher bedienen. So übernehmen zum Beispiel Dienstleister arbeitsintensive Prozesse wie Zahlungsabwicklung, Kundensupport und Lösegeldwäsche in Kryptowährungen.

Die zunehmende Verbreitung von Kryptowährungen wie Bitcoin oder Monero hat wiederum einen großen Einfluss auf die Cyber-Kriminalität. Derzeit werden rund 98 % aller Ransomware-Lösegelder in Bitcoin bezahlt. Während derlei Zahlungen in den 2000er Jahren noch über obskure und umständliche Dienstleister abgewickelt wurden, existiert heute mit Kryptowährungen eine einfache, weit verbreitete und halbwegs sichere digitale Zahlungsform. Die bisherigen, weitgehend unregulierten Kryptowährungen erleichtern Geldwäsche, einige von ihnen, insbesondere Monero, erschweren die Nachverfolgung von Finanzströmen.

Hinzu kommt, dass die Preise enorm gefallen sind. Eine Ransomwarekampagne kann schon für wenige hundert bis tausend Euro lanciert werden, so eine Studie von Deloitte. Dagegen kosten defensive Maßnahmen der IT-Sicherheit oft bedeutend mehr, im Schnitt 0,48 % des Jahresumsatzes bzw. rund 7 % der IT-Etats von Unternehmen. Angreifer sind also allein schon aufgrund geringer Kosten im Vorteil.

Die einfache Verfügbarkeit führt zu einer Proliferation von Ransomware: Dank niedriger Preise können auch weniger professionelle Kriminelle mächtige Angriffswerkzeuge einkaufen und einsetzen. Einer Vielzahl von Akteuren, denen andernfalls das Know-how fehlen würde, ist es insofern möglich, komplexe, potenziell sehr kostspielige und gefährliche Cyber-Angriffe auszuführen, etwa gegen kritische Infrastrukturen wie Wasserwerke. Denkbar ist auch, dass Staaten solche Dienste anmieten, um Spuren zu verwischen, und beispielsweise einzelne Dienste bzw. Malwarekomponenten für eigene Cyber-Angriffe verwenden, so geschehen bei dem NotPetya-Angriff durch Russland im Jahr 2017. Auch das wirtschaftlich sanktionierte Nordkorea setzt vermutlich staatliche Angreifer ein, um mit Ransomware seinen Staatshaushalt aufzubessern. Es lässt sich nicht ausschließen, dass andere ökonomisch benachteiligte Staaten dieses Modell vermehrt imitieren, etwa um Wirtschaftssanktionen zu unterlaufen. Ebenso ist vorstellbar, dass Ransomware als ökonomische Waffe (»denial of business attack«) eingesetzt wird mit dem Ziel, Konkurrenzunternehmen in Existenznöte zu bringen.

Sozioökonomische Dimension

Dass Ransomware momentan so viel Erfolg hat, ist auch Folge des Fachkräftemangels in der IT-Sicherheitsbranche. Laut einer Studie von Trend Micro (2019) fehlen in 56 % der deutschen Unternehmen solche Fachkräfte. Europaweit sind 168.000 Stellen unbesetzt, etwas weniger als in den Jahren

zuvor. Dieser Mangel führt zu einem Anstieg der Löhne für Expertinnen und Experten, mit der Folge, dass sich viele kleinere, aber kritische Organisationen kein spezialisiertes IT-Sicherheitspersonal für präventive Schutzmaßnahmen gegen Ransomware leisten können.

Der Mangel ist ein Problem nicht nur bei der Prävention, sondern auch bei der Reaktion. Es gibt nicht genügend »Incident Responder«, die helfen können, von Ransomware befallene Systeme wiederherzustellen. Existierende Dienstleister sind schnell ausgelastet, wenn eine neue Ransomware-Welle gleichzeitig viele potenzielle Kunden erfasst. Sie müssen dann unangenehme »Cyber-Triage« praktizieren. Sind also viele Organisationen parallel betroffen, lässt sich im Zweifelsfall nicht allen rechtzeitig helfen. Das kann im schlimmsten Fall kaskadierende Effekte produzieren.

Während also einerseits ein Mangel an IT-Sicherheitspersonal herrscht, gibt es andererseits immer mehr Angreifer. Laut einer Studie von Carbon Black ist die Zahl der Akteure in der Ransomware-Untergrundökonomie in den letzten Jahren rapide gewachsen. Mittels Ransomware kann man schnell reich werden, was insbesondere für Kriminelle in Regionen mit geringen Entwicklungschancen attraktiv ist. Ransomware-Gruppen rekrutieren aktiv und global IT-Fachkräfte, denen sie teils höhere Einkommen bieten als der legale Markt.

Manche Forschungsergebnisse deuten darauf hin, dass Cyber-Kriminalität mit dem sozioökonomischen Status korreliert: Insbesondere in sozioökonomisch schwachen Regionen und Ländern mit guten Bildungssystemen, in denen gleichzeitig die Staatlichkeit schwach ausgeprägt ist, finden sich häufig Cyber-Kriminelle. Korruption und fehlendes investigatives Know-how auf staatlicher Seite tragen zudem oft dazu bei, dass lokale Strafverfolger das Problem entweder nicht sehen können oder darüber hinwegsehen, bei aufgehaltener Hand. Folglich werden diese Staaten zum sicheren Hafen für Kriminelle, die sie vor Auslieferung schützen. Die USA beschuldigen Russland mittlerweile offen, ein solcher »cyber safe haven« zu sein; denn russische Nachrichtendienste pflegen angeblich Beziehungen mit Cyber-Kriminellen und kooperieren teils auch direkt mit ihnen. Unter russischsprachigen Cyber-Kriminellen gilt seit Jahren eine Art Kodex, keine russischen Ziele anzugreifen, sondern sich auf westliche Staaten zu konzentrieren. Andere autoritäre Staaten profitieren ebenfalls von heimischen Cyber-Kriminellen und lassen sie daher unbehelligt gewähren: Staaten setzen diese stellvertretend in ihren Cyber-Operationen »unter falscher Flagge« ein. So können sie plausibel die eigene Beteiligung abstreiten. Kriminelle haben die Möglichkeit, dem Staat direkt oder eher indirekt auf Auftragsbasis zuzuarbeiten. In den entsprechenden Regionen müssen sie nicht mit Strafverfolgung rechnen. Oftmals existieren auch keine Auslieferungsabkommen mit westlichen Staaten.

Ransomware ist also nicht nur ein technisches, sondern auch ein soziales und wirtschaftliches Problem, das mit zunehmender globaler Ungleichheit und fortschreitender digitaler Vernetzung eher größer als kleiner werden dürfte.

Technische Maßnahmen

Bisherige staatliche Versuche, Ransomware zu bekämpfen, sind vorwiegend technischer Natur. Diverse Cyber-Behörden wie das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Cybersecurity & Infrastructure Security Agency (CISA) in den USA informieren seit Jahren über bekannte und etablierte »best practices« zur Prävention. Diese umfassen: technische Maßnahmen wie Patch- und Schwachstellenmanagement in IT-Abteilungen, die Systeme so up to date halten; Netzwerkmonitoring und Detektion, die alle Systeme im Netzwerk sichtbar machen und Anomalien erkennen lassen; das Vorhalten dezentraler, regelmäßiger »off-site«-Backups, die nicht mit operativen Systemen verbunden sind, um deren Infektion zu vermeiden; segmentierte und isolierte Netzwerk-Topografien, die verhindern, dass Mal-

ware sich ungehindert in einer Firma ausbreiten kann; Zugangskontrollmanagement, das nur denjenigen Zugriff auf administrative Funktionen erlaubt, wenn diese akut gebraucht werden; das Abschalten unnötiger Wartungsverbindungen wie das Remote Desktop Protocol; das Einrichten einer Zwei-Faktor-Authentifizierung bei Diensten, die über das Internet erreichbar sind (Mail, Clouds etc.); »allow-listing« von Anwendungen, was das Starten unerlaubter Schadsoftware in Anhängen unterbindet; regelmäßige Trainings wie Email-Hygiene und Awareness, die Nutzerinnen und Nutzer dazu anhalten, nicht auf verdächtige Anhänge zu klicken.

Diese Maßnahmen sind zwar hinlänglich bekannt, werden meist aber von Organisationen nicht befolgt oder gar fehlerhaft umgesetzt. Viele Unternehmen — das gilt inzwischen vielfach auch für öffentliche Verwaltungen, Universitäten oder Krankenhäuser — machen diese grundlegenden Hausaufgaben nicht. Dafür gibt es vielerlei Gründe. Kosten sind ein Faktor, fehlendes Problembewusstsein bei Entscheidern ein weiterer. Noch immer sind die Ausgaben für IT-Sicherheit zu gering. Laut einer Umfrage des Branchenverbands Bitkom geben nur rund 31 % der deutschen Unternehmen nach dem empfohlenen Richtwert rund 20 % ihrer IT-Haushaltsmittel für IT-Sicherheit aus. Nicht selten wird immer noch fälschlich angenommen, dass die eigene Organisation nicht interessant genug ist und darum nicht betroffen sein wird. Folglich sind viele IT-Abteilungen nicht angemessen finanziert und unterbesetzt. Häufig werden die IT-Arbeitsstunden und -Personalstellen vollständig für den »Desk Support« und den Betrieb von IT-Systemen verwendet.

Für die präventive Vorsorge und die Entwicklung von Notfallstrategien fehlen häufig Zeit und Geld, die investiert werden müssten, um mit immer besser werdenden Angreifern Schritt zu halten. IT-Sicherheit hat wie Gesundheitspolitik oder Katastrophenschutz mit dem Präventionsparadox zu kämpfen: Gibt man Millionen für Präventionsmaßnahmen aus und passiert lange Zeit nichts, stellt sich rasch die Frage, ob diese Summen nicht eingespart werden können. Entscheiderinnen und Entscheidern fehlt auch oft das Bewusstsein dafür, dass für IT-Sicherheit eine spezifische Ausbildung oder Schulung und Fachwissen nötig sind, woran es dem eigenen IT-Personal vielfach mangelt.

Abgesehen von den Defiziten bei Präventionsmaßnahmen wäre es darüber hinaus erforderlich, dass Organisationen Notfallstrategien und Recovery-Pläne entwickeln. Das würde die Cyber-Resilienz erhöhen. Reaktionspläne müssen methodisch durchdacht sein und verschiedene Szenarien bzw. Ausfälle diverser Systeme antizipieren: Wie dämmt man die Verbreitung von Schadsoftware im Netzwerk ein und schützt Systeme, die vielleicht noch nicht betroffen sind? Wie sichert man Spuren für eine spätere forensische Analyse? Wie dokumentiert man Entscheidungen, die im Notfallmodus getroffen werden, im Nachgang aber noch rekonstruierbar sein sollen?

Außerdem muss es eine Backup- und Wiederherstellungsstrategie geben. Denn das Einspielen von Backups in großen, eventuell global verteilten IT-Umgebungen ist ein komplexes Unterfangen. Dies kann aufgrund großer Datenmengen sehr lange dauern, wahrscheinlich ist nach der Backup-Einspielung auch hoher Administrationsaufwand zu treiben, um kleinere Fehler zu beheben. Deswegen sollten derlei Reaktionspläne regelmäßig eingeübt werden.

Zur Notfallplanung gehört auch eine Strategie für die Kommunikation nach innen und außen. Wie erreicht man IT-Personal, das eventuell im Urlaub oder Wochenende ist? Cyber-Angriffe korrelieren mit Feiertagen. Wie geht man mit Medienanfragen um, die zu erwarten sind? Was kommuniziert man den Kunden? Ferner sind Kontinuitätspläne erforderlich, die definieren, welche grundlegenden Organisationsfunktionen im Minimalbetrieb aufrechtzuerhalten sind, nachdem es zu einem Befall durch Ransomware gekommen ist. Vielen Unternehmen würde der wirtschaftliche Bankrott drohen, wenn für Monate Buchungssysteme oder Dienstleistungen für die Kundschaft nicht mehr funktionieren.

Eine allgemeine politische Verpflichtung zu elementaren Schutzmaßnahmen gibt es indes nicht. Lediglich Betreiber von Infrastrukturen, die für die Versorgung hochgradig kritisch sind, müssen bestimmte »technische und organisatorische Maßnahmen« (nach ISO 2700X) treffen. Die breite Masse der kleinen und mittelständischen Unternehmen muss zwar Brandschutz-, Datenschutz- und Gesundheitsschutzpläne vorhalten; IT-Schutz und Vorsorgepläne sind in Deutschland aber nicht weithin verpflichtend. Daher sollte über gesetzlich verpflichtende Notfall- und Vorsorgestrategien nachgedacht werden, die sektorenspezifisch angelegt bzw. an der Unternehmensgröße orientiert sind. Ein IT-Sicherheitsfonds nach australischem Vorbild könnte kleinere Organisationen entlasten, die sich solche IT-Sicherheitsmaßnahmen kaum leisten können.

Maßnahmen anderer Länder

Die USA verlassen sich bei der Bekämpfung von Ransomware mittlerweile nicht mehr nur auf technisch-präventive Maßnahmen. Präsident Joe Biden hat diesen Kampf politisch ähnlich hoch priorisiert wie die Terrorismusbekämpfung. Im Juli 2021 wurde eine behördenübergreifende Ransomware Task Force gegründet, die das Problem mit einem »whole of government«-Ansatz angehen soll. Die zentral koordinierte Task Force erfasst alle Ransomware-Vorfälle und -Ermittlungen in den USA und bündelt die wichtigsten Informationen, um ein vollständiges Lagebild zu erstellen. Dazu gehören Informationen über Angreifer, die genutzte Schadsoftware, die dabei verwendete Infrastruktur (insbesondere Botnetze und Bullet-Proof-Hosting-Dienste), über Opfer und Lösegeldtransaktionen. Weiterhin werden Informationen zur Untergrundökonomie gesammelt, konkret zu den Foren im Darknet, zu Ransomware-as-service-Plattformen und zu Blogs von Ransomwaregruppen. Dabei werden auch nachrichtendienstliche und »Open Source Intelligence«-Verfahren angewendet (vgl. SWP-Aktuell 28/2019).

Darüber hinaus werden Zahlungsströme in den Blick genommen. Bisher fehlt ein Überblick, an wen bzw. an welche Bitcoin-Konten Unternehmen in den USA ihre Lösegeldzahlungen entrichten, was die Nachverfolgung erschwert. Finanztransaktionen über Bitcoin werden mittels Blockchain-Technologie gespeichert und sind daher im Prinzip nachverfolgbar. Diesen Umstand will sich auch Australien zunutze machen, wo kürzlich ein Entwurf für ein Gesetz vorgestellt wurde, das Unternehmen verpflichten soll, etwaige Ransomware-Zahlungen an das australische Cyber Security Centre zu melden. In den USA soll überdies eine neue öffentlich-private Partnerschaft zwischen Industrie und Finanzministerium Krypto-Zahlungsströme in Echtzeit überwachen. Das US-Finanzministerium entwickelt zudem neue Regularien für Betreiber von Krypto-Währungsexchanges — jenen Stellen, die digitale in analoge Währungen umtauschen — und für »over the counter trading desks«, die auf diese Weise an bestehende Anti-Geldwäscheverfahren der analogen Finanzindustrie gebunden werden sollen. Dazu gehören »know your customer«-Prozesse, die Exchanges dazu verpflichten, die Identitäten von Konteninhabern zu überprüfen, sowie das Befolgen von Anti-Geldwäsche- bzw. Antiterror-Finanzierungsgesetzen. Außerdem sollen Krypto-Exchanges künftig Auszahlungen ab 10.000 US-Dollar an Aufsichtsbehörden melden.

Das Problem ist, dass diese Regelungen nur heimische Exchanges betreffen, nicht aber ähnliche Services im Ausland. Wahrscheinlich werden Kriminelle dann auch auf andere Kryptowährungen wie Monero ausweichen, die schwerer zu überwachen sind. Insofern kann das Ziel nur sein, Transaktionen zu erschweren, die sich vollständig nie werden verhindern lassen. In Großbritannien wird unterdessen die Idee diskutiert, Ransomware-Zahlungen Betroffener gänzlich zu verbieten, um den Kriminellen die Geschäftsgrundlage zu entziehen. Der Vorschlag ist insofern kontrovers, als sich nicht wenige Unternehmen vor der Entscheidung sehen, entweder die Lösegeldforderung zu erfüllen oder Insolvenz

anzumelden. Auch wenn in der IT-Sicherheitsindustrie die Maxime gepredigt wird, »zahle nicht das Lösegeld«, weil damit das kriminelle Ökosystem und die Entwicklung neuer Angriffstechniken unterstützt werden, ist sie häufig nicht praktikabel.

Multilaterale Maßnahmen

Da Regularien für Kryptowährungsdienstleister national nur begrenzt wirksam sind, müssen sie international in multilateralen Foren durchgesetzt werden. Beim G7-Treffen im Sommer 2021 wurde das Thema erstmals angesprochen. Allerdings lag der Fokus vor allem darauf, dass Staaten es nicht wissentlich dulden sollten, Kriminelle von ihrem Territorium aus operieren zu lassen. Sie sollten vielmehr ihrer Sorgfaltsverantwortung nachkommen und die kriminellen Machenschaften stoppen und verfolgen, sofern sie von ihnen wissen oder von anderen Staaten Hinweise bekommen. Auf diese Norm verantwortlichen Staatenverhaltens hatten sich die UN-Mitglieder vor einigen Jahren geeignet, allerdings ist sie nicht verbindlich, sondern nur freiwillig einzuhalten. Die Kooperation bei der Regulierung von Digitalwährungen stand beim G7-Treffen nicht im Vordergrund, wird aber im Rahmen der Financial Action Task Force ein Thema sein, die internationale Standards und Instrumente zur Kontrolle virtueller Währungen entwickeln soll.

Krpytowährungsdienste sind jedoch nur ein Teil des Problems. Ein anderer sind die Auswüchse der Ransomware-Untergrundökonomien, zu deren Einhegung die Staaten einen strukturierten Ansatz entwickeln sollten, indem sie sich etwa verpflichten, keine Bullet-Proof-Hosting-Dienste auf ihrem Territorium zuzulassen bzw. strafrechtlich gegen sie vorzugehen. Da Anti-Geldwäscheprozesse allerlei Schlupflöcher bieten, hat eine Gruppe internationaler Forscher auf dem World Economic Forum 2021 einen »Zuckerbrot und Peitsche«-Ansatz vorgeschlagen, um auf Staaten einzuwirken, die Ransomware-Aktivitäten auf ihrem Territorium dulden. Dabei soll die ganze Bandbreite außenpolitischer Maßnahmen genutzt werden, inklusive »naming & shaming« in öffentlichen Foren, die Androhung, finanzielle Unterstützung und Entwicklungshilfe zu kürzen, bis hin zu Wirtschaftssanktionen. Wo Ermittlungskapazitäten fehlen, sollten fortschrittlichere Staaten unterstützend eingreifen und »capacity building« in Drittländern betreiben, um Strafverfolger zu wirksamem Handeln zu befähigen. Flankierend bietet das US-Außenministerium jenen als Anreiz Belohnungen von bis zu 10 Millionen US-Dollar an, die US-Behörden Tipps zur Identifizierung staatlich gestützter Cyber-Angriffe auf kritische Infrastrukturen geben. Hier wird exemplarisch und in vorbildlicher Weise ein breites Instrumentarium staatlichen Handelns eingesetzt. Der erhöhte Druck der US-Regierung scheint zumindest momentan zu wirken: Nachdem US-Präsident Biden das Thema bei Russlands Präsident Putin angesprochen hatte, gingen die Aktivitäten der Ransomware-Gruppe REvil zurück. Ob dies aber an den bilateralen Konsultationen lag oder andere Gründe hatte, wie etwa eine verborgene Offensive von U.S. Cyber Command, ist unklar. Außerdem muss sich erst zeigen, ob die Gruppe ihre Aktivitäten dauerhaft eingeschränkt hat oder nur kurzfristig die Füße stillhält, bis der öffentliche Druck nachgelassen hat.

Darüber hinaus sollten Bemühungen intensiviert werden, Russland und die Mitglieder der Gemeinschaft Unabhängiger Staaten (GUS) zu bewegen, der völkerrechtlich bindenden Budapest-Konvention gegen Cyber-Kriminalität beizutreten, die seit 2004 in Kraft ist und von 46 Staaten ratifiziert wurde. Diese Konvention regelt zum Beispiel Fragen länderübergreifender Strafverfolgung und den Austausch elektronischer Beweismittel bei Ermittlungen gegen Cyber-Kriminalität. Russland verweigerte seinerzeit den Beitritt, weil es in den Bestimmungen eine Einmischung in innere Angelegenheiten sah. Seitdem versucht das Land auf UN-Ebene, die Budapest-Konvention durch ein eigenes Cybercrime-Regime zu ersetzen, das diverse Maßnahmen zur Zensur von Internetinhalten ebenso vor-

sieht wie Einschränkungen eines freien, globalen Internets. Für demokratische Staaten ist das eine rote Linie, die nicht überschritten werden sollte. Da auch die Budapest-Konvention Defizite hat und über Reformen nachgedacht wird, sollte Russland hier mit an den Tisch geholt werden. Gleichzeitig gilt es Anreize zu schaffen, dass Russland einem reformierten Vertrag beitritt, an dessen Reform es mitwirken könnte.

Offensive Maßnahmen?

Nicht zuletzt stellt sich die Frage, inwiefern eigene offensive Cyber-Maßnahmen gegen die Ransomware-Kommandoinfrastruktur gerichtet werden können und sollten. Das U.S. Cyber Command nutzte Cyber-Operationen, um die Infrastruktur des Trickbot-Botnetzes temporär zu stören. Das gab Anlass zu einer Diskussion darüber, ob eine Militarisierung dieses gesamtgesellschaftlichen Problems der richtige Ansatz ist. Militärische Maßnahmen sollten immer die letzte Wahl bleiben, und vor ihrem Einsatz sollte ihre Notwendigkeit sorgfältig geprüft werden, so der US-Politologe Jason Healey. Denn notwendig dürften sie nur in nur sehr wenigen Fällen sein, etwa bei direkter Involvierung eines anderen Staates.

Darüber hinaus ist zu klären, was ein Gegenschlag bezwecken soll. Wenn das Ziel ist, Ransomware-Infrastruktur dauerhaft auszuschalten, dürfte dies kaum zu erreichen sein, wie das Trickbot-Beispiel zeigt: Nur wenige Wochen nach dem Gegenschlag waren die Kriminellen mit einem neuen Botnet wieder aktiv. Das Untergrundökosystem ist mit anderen Worten überaus effektiv und resilient, Ausweichmöglichkeiten lassen sich sehr schnell wiederaufbauen oder anmieten. Cyber-Spionageoperationen, mit denen Kommandoinfrastruktur infiltriert werden sollen, können in Einzelfällen aber Informationen über verwendete Schadsoftware oder Betreiber bzw. Servicedienstleister liefern, sofern sie ihre Spuren nicht gut verwischen. Solche Operationen scheinen darum eher für die Strafverfolgung von Nutzen zu sein.

Cyber-Operationen, die der Immunisierung (»Zwangsimpfen«) von mit Schadsoftware infizierten Endgeräten der Opfer dienen sollen, wie sie im Falle des Emotet-Botnetzes diskutiert wurden, sind risikoreich. Es ist nie völlig klar, welche Kollateralschäden ein Eingriff in die Integrität von Systemen anrichten kann. Cyber-Gegenschläge sind also kein Wundermittel und können allenfalls begleitend bei Strafverfolgungsermittlungen eine Rolle spielen. Dazu müssen sie in Kombination mit den angesprochenen anderen Instrumenten in eine umfassende Strategie eingebettet sein. Nationale Ad-hoc-Alleingänge sind dabei wenig hilfreich, da Cyber-Operationen im schlimmsten Fall die Ermittlungsbemühungen anderer Länder torpedieren. Insofern muss über international abgestimmte Mechanismen nachgedacht werden. Hierfür sind eine sorgfältige und systematische Analyse potenzieller Schadenseffekte und gegebenenfalls die Aufstellung von Mitigations- bzw. Kontingenzplänen zwingend erforderlich. Für deutsche Behörden stellen sich bei einem solchen Vorgehen diverse grundrechtliche Fragen.

Fazit

Die nächste Bundesregierung sollte prüfen, welche der hier diskutierten Maßnahmen auch in Deutschland umgesetzt werden könnten. Sehr wichtig wäre, dass das Thema höher priorisiert und geeignete Konzepte und Maßnahmen gesamtstaatlich koordiniert werden. Dazu braucht es ein Lagebild über die Untergrundökonomie und die Zahlungsströme. Darüber hinaus ist die Unterstützung multilateraler Initiativen sinnvoll, die gegen das Untergrundökosystem vorgehen; dazu gehört etwa die Finanzregulierung von Kryptowährungsdiensten. All dies wird aber nur begrenzte Wirksamkeit entfalten, solange Organisationen in Deutschland nicht stärker verpflichtet bzw. dabei unterstützt werden, ihre IT-Sicherheitshausaufgaben zu machen.

Dr. Matthias Schulze ist Stellvertretender Leiter der Forschungsgruppe Sicherheitspolitik.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
doi: 10.18449/2021A56