Alina Boll

Ohne Cybersicherheit kein Datenschutz, ohne Datenschutz keine Cybersicherheit?

Wiederherstellen der Cybersicherheit durch aktive Abwehr von Cyberangriffen[1]

Der Schutz personenbezogener Daten setzt die Sicherheit der Datenverarbeitung voraus. Datensicherheit ist damit integraler Bestandteil und sogar Voraussetzung für einen effektiven Datenschutz. Aber auch Cybersicherheitsmaßnahmen müssen sich an datenschutzrechtliche Vorgaben der DSGVO halten, sofern im Rahmen dessen personenbezogene Daten verarbeitet werden. Ob und wie der Datenschutz bei der Ausführung einer Cybersicherheitsmaßnahme durch IT-Sicherheitsforschungseinrichtungen umzusetzen ist, erläutert dieser Artikel anhand der Verteidigung eines BGP-Hijacking Angriffs.

1 Problemstellung

Politisch, militärisch sowie kriminell motivierte Cyberangriffe gegen (Bundes-)Behörden, Politik und Wirtschaftsunternehmen sind seit Jahrzehnten eine real drohende Gefahr.[2] Unter „Cyberangriffen" versteht man gezielte Maßnahmen gegen Infrastrukturen der Informationstechnologie, die entweder der Informationsbeschaffung – insbesondere von Kundendaten oder Geschäftsgeheimnissen – oder der Schädigung bzw. Sabotage des angegriffenen IT-Systems dienen.[3] Im Zuge der Digitalisierung und der damit einhergehenden digitalen Vernetzung ist die Zahl der Cyberangriffe erheblich gestiegen. So ergab eine im Jahr 2022 durchgeführte Umfrage, dass rund 46 Prozent der befragten Unternehmen in Deutschland mindestens einmal Opfer einer Cyber-Attacke wurden.[4] Nicht zuletzt durch den Ukrainekrieg und eine hybride Kriegsführung auch im digitalen Raum ist die Bedrohung durch Cyberattacken für die Wirtschaft und Politik real geworden und zeigt, dass die Gefährdungslage im Cyber-Raum so hoch wie nie ist.[5] Auch die Ziele der Cyberkriminellen haben sich im Laufe der Zeit erweitert, so ist neben öffentlichen Einrichtungen, dem Gesundheits- und dem Bildungssektor, dem E-Commerce sowie Kritischen Infrastrukturen nahezu jede Branche im Jahr 2021 Opfer von Cyberangriffen geworden.[6] Damit wird fast jedes Unternehmen in Deutschland (potenziell) Ziel von Cyberangriffen. Laut dem Branchenverband Bitkom e.V. waren im Jahr 2021 84 % der deutschen Unternehmen von Cyberangriffen betroffen und weitere 9 % gehen davon aus, betroffen gewesen zu sein.[7] Den Angreifern geht es dabei überwiegend um Spionage, Erpressung und Identitätsdiebstahl sowie die Sabotage, Zerstörung und Stilllegung von IT-Systemen.[8]

1.1 Aktive Cyberabwehr – keine Hackbacks

Um Cyberangriffe zu vermeiden, gilt es, die eigene IT kontinuierlich durch technische und organisatorische Maßnahmen nach dem neuesten Stand der Technik abzusichern. Die stetig steigende Zahl der Cyberangriffe und die neue Bedrohungslage durch Cyberangriffe im Zusammenhang mit dem Ukrainekrieg zeigen jedoch, dass technische und organisatorische Maßnahmen zur Prävention von Cyberangriffen nicht der einzige Weg zur Absiche-

1 Diese Forschungsarbeit wurden vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der vorliegende Beitrag gibt die persönliche Meinung der Autorin wieder.

2 *BMI*, https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html.

3 *Schmidt-Versteyl*, Cyber Risks – neuer Brennpunkt Managerhaftung?, NJW 2019, 1637 (1637).

Alina Boll

ist wissenschaftliche Mitarbeiterin der Abteilung IT Law & Interdisciplinary Privacy Research am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) und am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.
E-Mail: alina.boll@sit.fraunhofer.de

4 *Statista,* https://de.statista.com/statistik/daten/studie/1230157/umfrage/unternehmen-die-in-den-letzten-12-monaten-eine-cyber-attacke-erlebt-haben.

5 *BSI,* Die Lage der IT-Sicherheit in Deutschland 2022. S. 7; https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.

6 *BKA,* Cybercrime, Bundeslagebild 2021, S. 1.

7 *Bitkom e.V.*, 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen, Berlin 2022, https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.

8 *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, S. 4.

rung gegen Cyberangriffe sein sollten. Als Ergänzung wird vor allem das Stoppen und Verhindern von Cyberangriffen durch Maßnahmen der aktiven Cyberabwehr diskutiert. Unter Maßnahmen der aktiven Cyberabwehr sind hier nach *Shulman und Waidner* keinesfalls „*digitale Vergeltungsangriffe im Sinne von „Hackbacks"* [9] *oder die Cyberfähigkeit der Bundeswehr*" zu verstehen, sondern vielmehr „*technische Maßnahmen, die Angriffe stoppen oder proaktiv verhindern sollen, indem sie in die Infrastrukturen oder digitalen Ressourcen der Angreifer eingreifen*". Ziel ist die Unterstützung der Strafverfolgungs- und Gefahrenabwehrbehörden bei der Vereitelung und Verfolgung von Cyberangriffen.[10]

1.2 Widerherstellung des Internetverkehrs

Aktive Cyberabwehr kommt bspw. dann zum Einsatz, wenn böswillige Angreifer den Internetverkehr manipulieren. Die Beeinflussung des Internetverkehrs spielt vor allem bei dem sog. BGP-Hijacking Angriff eine Rolle, bei welchem Angreifer den Internetverkehr böswillig über die eigenen Server umleiten.[11] Ziel des Angriffs ist es insbesondere, Daten abzufangen, zu überwachen und/oder den externen Datenverkehr des Angegriffenen nahezu vollständig stillzulegen. So wurde bspw. im Juni 2022 der für das Unternehmen Apple Inc. bestimmte Internetverkehr für 12 Stunden durch den russischen Provider Rostelecom über dessen Server in Russland umgeleitet.[12] Zwar ist im konkreten Fall aufgrund der Verschlüsselung des Datenverkehrs zwischen Apple Geräten und Apple Servern vermutlich kein (größerer) Schaden für das Unternehmen und seine Kunden entstanden. Gleichwohl kann sich ein solcher Angriff jederzeit wiederholen und auch gegen andere Organisationen und/oder unverschlüsselte Verbindungen richten. So hat ebenfalls ein russischer Provider im Jahr 2018 einen Teil des zu Amazon gehörenden Datenverkehrs gekapert, sodass Nutzer zu einer gefälschten und von Hackern kontrollierten Website umgeleitet und in der Folge etwa 152.000 USD in Kryptowährung gestohlen wurden.[13]

Derartige Angriffe können durch die Wiederherstellung des (rechtmäßigen) Internetverkehrs als Maßnahme aktiver Cyberabwehr gestoppt werden. Dieses Vorgehen soll im Folgenden zunächst technisch erörtert werden. Anschließend sollen die Chancen, aber auch die Risiken aufgezeigt werden, die eine Widerherstellung des Internetverkehrs als Maßnahme der aktiven Cybersicherheit für die Informationssicherheit und den Datenschutz mit sich bringt.

2 Technische Grundlage des BGP-Hijacking und dessen aktiver Abwehr

Das Internet setzt sich aus einer Reihe von großen Netzwerken zusammen, sogenannten *Autonomen Systemen* (AS), die von bestimmten Organisationen, überwiegend von Internet Service Providern (ISP), verwaltet und betrieben werden. Jedes AS kontrolliert dabei einen oder mehrere zusammenhängende Blöcke von IP-Adressen[14], *sog. IP-Präfix*,[15] und steht dabei mit einem oder mehreren AS über *sog. BGP-Router* in Verbindung.[16] Über das *Border-Gateway-Protokoll (BGP)* melden alle AS die Netzwerke, mit denen sie verbunden sind und zu denen sie als Verbindungsnetz Daten weiterleiten können.[17] Mittels BGP wird dynamisch der gesamte „Postweg" *(sog. Routen)* von einem BGP-Router eines AS zu jedem BGP-Router eines anderen AS veröffentlicht und in Tabellen gespeichert, den sog. *BGP-Routingtabellen*.[18] Da sich die Struktur des Internets ständig ändert, neue AS hinzukommen und andere nicht mehr verfügbar sind, kann jeder BGP-Router gegenüber seinen benachbarten BPG-Routern *Update-Nachrichten (sog. Announcements)* verbreiten, in welchen er mitteilt, für welche Ziel-IP-Präfixe er eine gute und effiziente Route kennt.[19] Der BGP-Router soll folglich dafür sorgen, dass Datenpakete möglichst effizient, über die beste Route, ihr jeweiliges Ziel-AS erreichen. Die Update-Nachrichten werden i.d.R. von allen weiteren benachbarten BGP-Routern ohne Überprüfung ihrer Richtigkeit übernommen.[20] Untechnisch gesprochen gibt es also niemanden, der überprüft, ob der Postbote den richtigen Weg zum Adressaten kennt. Der einzige Weg, um festzustellen, ob die Wegbeschreibung böswillig verändert wurde, wäre die Beobachtung, dass viele Briefe in den falschen Briefkasten ankommen.

Bei einem BGP-Hijacking Angriff kann der Angreifer also vergleichsweise einfach IP-Präfixe seiner Opfer übernehmen, indem er fälschlicherweise in einer Update-Nachricht den Besitz des IP-Präfixes seines Opfers behauptet.[21] Untechnisch gesprochen behauptet der Angreifer also, dass er die Post-Adresse des Opfers besitzt und fängt somit dessen Briefe ab. Dies kann der Angreifer so einfach machen, da das BGP auf jegliche Sicherheitskontrollen verzichtet und allein darauf vertraut, dass miteinander verbundene Netzwerke die Wahrheit darüber sagen, welche IP-Adressen sie besitzen.[22] Akzeptiert der BGP-Router diese Update-Nachricht, hat dies zur Folge, dass er eine falsche Route in seine Routingtabelle übernimmt, weiterverteilt und diese in der Folge auch von anderen BGP-Routern übernommen wird. In der Konsequenz des BGP-Hijackings wird der Internet-Verkehr des Opfers umgeleitet, sodass ihn der Angreifer leicht überwachen und/oder sogar abfangen kann.[23]

Eine effektive Verteidigungsmaßnahme besteht nun darin, den IT-Sicherheitsforschenden – nachdem er einen Teil des gehijackten IP-Präfix des Opfers kennt – eine korrigierende Up-

9 Bei einem sog. Hackback geht es darum, bei großangelegten Attacken – etwa auf wichtiger Infrastruktur – in ausländische Server einzudringen, um diese, im Sinne eines digitalen Gegenschlags, lahmzulegen.

10 Vgl. zum Ganzen: *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, S. 3 ff.

11 *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, S. 6.

12 *Pfister,* russischer Provider kapert Apple-Adressraum, https://www.heise.de/news/Russischer-Provider-kapert-Apple-Adressraum-7193705.html.

13 https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency/.

14 Eine IP-Adresse ist eine eindeutige und individuell zugeteilte Anschlussnummer eines jeden Gerätes im Internet. Die IP-Adresse identifiziert damit jedes Gerät im Internet, damit es adressierbar und erreichbar ist (vergleichbar mit der Postanschrift auf einem Briefumschlag).

15 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage, S. 64.

16 Ebenda, S. 880.

17 Ebenda, S. 817.

18 Ebenda S. 64 Rn. 153.

19 Vgl. dazu: *Dierichs/Pohlmann*, Geordnetes Chaos, Wie Routing dem Internet Selbstheilungskräfte verleiht, c't 3/2006, 161 (162).

20 Fedler, Prefix Hijacking-Angriffe und Gegenmaßnahmen, S. 2 ff., https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf.

21 *Shulman/Waider,* FAZ, Deutschlands Sicherheit – Der Weg zur aktiven Cyberabwehr, S. 3, https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.

22 *Fedler,* Prefix Hijacking-Angriffe und Gegenmaßnahmen, S. 2, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf.

23 *Shulman/Waider,* FAZ, Deutschlands Sicherheit – Der Weg zur aktiven Cyberabwehr, S. 3, https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.

date-Nachricht an betroffene BGB-Router senden zu lassen, indem er das IP-Präfix des Opfers als zu diesem gehörig deklariert und die Falschinformation des Angreifers überschreibt. Akzeptiert und priorisiert der BGP-Router dieses Update, so ändern sich die Routen des Datenverkehrs wieder zu Gunsten des Opfers. Dieser wird folglich nicht mehr über oder gar zum Angreifer, sondern zurück zum Opfer gelenkt und der Angriff dadurch gestoppt.[24]

3 Chancen für die Informationssicherheit

Maßnahmen aktiver Cyberabwehr bieten erhebliche Chancen für die Informationssicherheit. Angriffe, wie das BGP-Hijacking, können abgewehrt und die Informationssicherheit der Angegriffenen wiederhergestellt werden. Eine Chance bieten sie insbesondere deshalb, weil erfolgreich durchgeführte Cyberangriffe i.d.R. mit weitreichenden finanziellen Schäden für die Angegriffenen einhergehen. Der Branchenverband Bitkom e.V. errechnete für das Jahr 2022 allein in Deutschland Cybercrime-Schäden in Höhe von rund 203 Mrd. Euro.[25] Dies resultiert insbesondere daraus, dass Cyberangriffe, wie das BGP-Hijacking, zu Ausfallzeiten, Datenverlusten oder Manipulationen und folglich zu umfassenden Serviceunterbrechungen und Produktivitätsverlusten führen.[26] Ein produzierendes Unternehmen ist dann ggfs. nicht in der Lage, die geplanten Aufträge fristgerecht und vollumfänglich abzuarbeiten, sodass Vertragsstrafen die Folge sein können.[27]

Durch Cyberangriffe entstehen den Unternehmen jedoch nicht nur substanzielle Schäden wie Umsatzeinbußen, Kosten für die Wiederherstellung der Betriebssysteme, Ursachenfeststellung und Hinzuziehung von juristischen und forensischen Beratern, auch Reputationsschäden können Folgen eines Cyberangriffs sein.[28] So kam es bspw. Ende 2013 bei einem der größten US-amerikanischen Einzelhändlern, der Target Corporation, zu einer gravierenden Sicherheitspanne. Cyberkriminelle hatten sich über Phishing-Angriffe auf einen Zulieferer der Target Corporation Zugangsdaten zu dessen Netzwerk verschafft und dort eine Malware in Point-of Sale-Systemen installiert. Diese lieferte den Angreifern Kredit- und Bankkartendaten von mehr als 40 Millionen Target-Kunden sowie mehr als 70 Millionen Adressdaten. Die direkten Folgeschäden dieses Angriffs beliefen sich auf rund 285 Millionen Euro. Aber auch die Reputation des Unternehmens wurde durch den Angriff nachhaltig in Mitleidenschaft gezogen. Die Konsumentenbewertung der Target Corporation, der sog. YouGov BrandIndex Buzz-Score[29], verzeichnete rapide Verluste. In den ersten Tagen nach dem Cyberangriff fiel der Wert von 22,4 auf -19 Punkte. Zwar ist es dem Unternehmen gelungen, den Wert in den folgenden Monaten etwas zu stabilisieren und anzuheben, doch auch 2019 hatte er, mit 18,5 Punkten, seinen ursprünglichen Wert nicht erreicht. In der Konsequenz des Reputationsverlustes wechselten zahlreiche Kunden zu Konkurrenzunternehmen, sodass Umsatz und Gewinn der Target Corporation nachhaltig einbrachen.[30]

Aufgrund dieser Gefahren gilt es, Cyberangriffe schnellstmöglich zu entdecken, zu verhindern und zu beheben. Um dieses Ziel zu erreichen, bedarf es einer starken IT-Sicherheitsforschung, die als neutral agierende Stelle rechtzeitig Schwachstellen, Risiken und stattfindende Angriffe aufzeigt, sowie auf deren Minimierung und Beseitigung hinwirkt.[31] Durch Maßnahmen aktiver Cyberabwehr – wie der Abwendung eines BGP-Hijacking Angriffs durch Widerherstellung des (rechtmäßigen) Internetverkehrs – können Schäden abgewehrt, der Eintritt weiterer Schäden vermieden und die Cybersicherheit der angegriffenen Unternehmen wiederhergestellt werden.

4 Risiken für die Informationssicherheit

Wenn auch die aktive Cyberabwehr in hohem Maße Chancen für die Informationssicherheit bietet, gilt es einen Aspekt zu berücksichtigen: Im Rahmen der aktiven Cyberabwehr, z.B. bei der Abwendung eines BGP-Hijacking-Angriffs durch IT-Sicherheitsforschungseinrichtungen, wird in der entsprechenden Forschungseinrichtung zwangsläufig die Information bekannt, welches Unternehmen Opfer eines Angriffs geworden ist. Die Information, welches Unternehmen angegriffen wurde und durch Cybersicherheitsforschende in der aktiven Abwehr des Angriffs unterstützt wurde, birgt daher ebenso Risiken für die Reputation und das Kundenvertrauen des angegriffenen Unternehmens.

Diese Informationen sind daher von IT-Sicherheitsforschenden grundsätzlich vertraulich bzw. verantwortungsvoll[32] zu behandeln. Auftraggeber aktiver Cyberabwehr sollten vor diesem Hintergrund vor einer Beauftragung die Notwendigkeit einer Vertraulichkeitsvereinbarungen prüfen, die Risiken für die Reputation des Auftraggebers minimieren kann.

5 Chancen für den Datenschutz

Anders als die Informationssicherheit hat der Datenschutz den Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten, den Schutz des Rechts auf informationelle Selbstbestimmung und den Schutz der Privatsphäre zum Ziel.[33] Überge-

24 *Ebenda.*

25 *Bitkom e.V.,* 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen, Berlin, 2022, https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.

26 Fedler, Prefix Hijacking-Angriffe und Gegenmaßnahmen, S. 3, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf.

27 *Bitkom e.V.*, Kosten eines Cyber-Schadensfalles-Leitfaden, 2016, S. 23.

28 *Schmidt-Versteyl*, Cyber Risks – neuer Brennpunkt Managerhaftung? NJW 2019, 1637 (1638); *Dittrich,* Geschäftsgeheimnisse im Visier von Cyberkriminellen – die Bedeutung der Cybersicherheit für den Geheimnisschutz in Unternehmen, NZWiSt 2023, 8 (9).

29 „Das Ranking basiert auf Daten des Markenmonitors YouGov BrandIndex, der tagesaktuell Informationen zu 16 Markendimensionen in den Bereichen Markenpräsenz, Markenbewertung und Markenbeziehung liefert. Für dieses Ranking wurde die Dimension „Buzz" betrachtet, welche auf der Frage: „Von welchen Marken haben Sie in den letzten zwei Wochen etwas Positives/Negatives gehört?" beruht. Der Buzz-Score ergibt sich aus dem Saldo der insgesamt abgegebenen positiven und negativen Bewertungen und kann somit auf einer Skala von -100 Punkten, bei ausschließlich negativen Bewertungen, bis +100 Punkten, bei ausschließlich positiven Bewertungen, liegen". https://yougov.de/topics/economy/articles-reports/2019/01/22/yougov-brandindex-buzz-jahresranking-dm-schafft-20°.

30 Zum Ganzen: *Guelstorff*, IT-Sicherheit richtig kommunizieren – Ansatzpunkt Unternehmensreputation, 2021, https://digitaleweltmagazin.de/it-sicherheit-richtig-kommunizieren-ansatzpunkt-unternehmensreputation/; https://www.handelsblatt.com/unternehmen/handel-konsumgueter/target-hackerangriff-kostet-us-handelskette-millionen/9543006.html.

31 *Balaban et. al*., Whitepaper zur Rechtslage der IT-Sicherheitsforschung, Version 1.0., S. 3.

32 Vor der Veröffentlichung von im Rahmen der IT-Sicherheitsforschung gefundener IT-Sicherheitsschwachstellen gilt es in diesem Zusammenhang z.B. die Best-Practice-Empfehlungen zum Coordinated Vulnerability Disclosure einzuhalten.

33 *Hornung/Spiecker gen. Döhmann,* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO, 1. Auflage 2019, Art. 1 Rn. 3.

ordnetes Schutzgut des Datenschutzes ist folglich die Wahrung der Grundrechte der hinter den Daten stehenden Menschen.[34] Dieses Schutzgut wird durch Cyberangriffe wie dem BGP-Hijacking-Angriff massiv gefährdet, so können die Angreifer bei Erfolg des Angriffs teilweise sehr umfangreich auf personenbezogene Daten zugreifen und u. a. erkennen, wann Kommunikation zwischen welchen Personen und aus welchem Grund stattgefunden hat; bei unverschlüsselter Kommunikation können Angreifer i.d.R. sogar die Inhaltsdaten der elektronischen Kommunikation einsehen. Aber auch verschlüsselte Daten könnten – jedoch mit einem erheblichen Aufwand – ggf. entschlüsselt und zu Lasten der betroffenen Personen ausgewertet oder verwendet werden.

Und auch neben dem BGP-Hijacking-Angriff ist der missbräuchliche Zugriff auf Daten häufiges Ziel von Cybersicherheitsangriffen. Laut Bitcom e.V. haben 68 % der im Jahr 2022 angegriffenen Unternehmen angegeben, dass im Rahmen von Cyberangriffen Kommunikationsdaten, wie E-Mails, entwendet wurden. Bei nahezu jedem zweiten betroffenen Unternehmen waren Kundendaten das Angriffsziel.[35] Unternehmen befürchten hierbei häufig, hohe Bußgelder auferlegt zu bekommen, die sich aus mangelnden Schutzmaßnahmen vor derartigen Cyberangriffen motivieren könnten. Auch Schadensersatzanforderungen betroffener Personen werden von den Unternehmen vor diesem Hintergrund befürchtet.[36] Nicht zu unterschätzen ist auch, dass durch den Angriff auf personenbezogene Daten Folgeangriffe und unberechtigte Datennutzungen drohen, die den betroffenen Personen wiederum einen nicht unerheblichen materiellen, aber auch immateriellen Schaden einbringen können.[37]

Die missbräuchliche Verwendung personenbezogener Daten kann durch Maßnahmen aktiver Cyberabwehr gestoppt und verhindert werden, wodurch in der Konsequenz auch Folgeschäden für die betroffenen Personen, wie bspw. ein Identitätsdiebstahl oder -betrug, ein finanzieller Verlust, eine Rufschädigung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, abgewendet und das Recht auf informationelle Selbstbestimmung geschützt werden kann.[38]

6 Risiken für den Datenschutz

Unterstützt eine IT-Sicherheitsforschungseinrichtung ein Unternehmen bei der Abwendung eines BGP-Hijacking Angriffs, so verarbeitet diese im Rahmen der Verteidigungsmaße nach oben beschriebenem Vorgehen neben den Daten, die zur Beauftragung der aktiven Cyberabwehr notwendig werden (i.d.R. Ansprechpartner und Kontaktdaten des angegriffenen Unternehmens), nur das IP-Präfix -- ggf. auch die gesamte(n) IP-Adresse(n) -- des angegriffenen Unternehmens. Regelmäßig bestehen daher durch die aktive Abwehr eines BGP-Hijacking keine besonderen Risiken des Datenschutzes.

7 Empfohlene Maßnahmen für Forschungseinrichtungen

Es bleibt festzuhalten, dass es in dem hier untersuchten Fall aus datenschutzrechtlicher Perspektive keine über den klassischen Kundendatenschutz (u.a. Eintrag zur Kundendatenverwaltung in das Verfahrensverzeichnis, Maßnahmen zur Umsetzung der Mandantentrennung, Maßnahmen zu Zutritts-, Zugangs- und Zugriffsschutz auf die Kundendaten) hinausgehenden datenschutzrechtliche Maßnahmen bedarf. Auch wird die IT-Sicherheitsforschungseinrichtung bei der *einmaligen* Abwendung eines Angriffs i.d.R. kein Auftragsverarbeiter des angegriffenen Unternehmens sein, sodass die speziellen Regelungen des Art. 28 ff. DSGVO keine Anwendung finden dürften. Unabhängig davon kann aufgrund des erörterten Reputationsrisikos der Abschluss einer Geheimhaltungsvereinbarung (sog. *Non-Disclosure Agreement, NDA*) zwischen der Forschungseinrichtung und dem angegriffenen Unternehmen sinnvoll sein. Wird ein NDA geschlossen, hat die Forschungseinrichtung wiederum dafür Sorge zu tragen, dass alle relevanten Mitarbeiter den Inhalt des NDA kennen und einhalten. Ggf. sind hierfür besondere Mitarbeiterschulungen umzusetzen.

8 Ausblick

Anders als bei dem hier erörterten Beispiel des BGP-Hijacking Angriffs erfordern einige andere aktive Cyberabwehrmaßnahmen ggf. deutlich mehr Verarbeitungen von personenbezogenen Daten durch IT-Sicherheitsforschungseinrichtungen. Hierbei ist insbesondere zu diskutieren, welche Ermächtigungsgrundlagen für die Verarbeitung von personenbezogenen Daten herangezogen werden können, wer Verantwortlicher im Sinne der DSGVO ist und ob die in der DSGVO enthaltenen Forschungsprivilegien in den konkreten Fällen Erleichterungen für IT-Sicherheitsforschungseinrichtungen mit sich bringen. Darüber hinaus gilt es für Forschungseinrichtungen die Grundsätze der DSGVO, wie etwa den Datenminimierungsgrundsatz, die Einhaltung technischer und organisatorischer Maßnahmen sowie die ggf. bestehende Durchführungspflicht einer Datenschutz-Folgenabschätzung einzuhalten.

Erschwerend ist in diesem Zusammenhang, dass es IT-Sicherheitsforschungseinrichtungen insbesondere während der Erforschung neuer Angriffsabwehrmethoden sowie bei deren erstmaligen Einsatz oftmals nur schwer möglich ist einzuschätzen, welche und wie viele personenbezogene Daten im Rahmen der Umsetzung der aktiven Verteidigungsmaßnahme erhoben werden. Hier bedarf es einer sorgfältigen Datenschutzvorsorge ohne genaue Kenntnisse der bevorstehenden Datenverarbeitung – einer im Bereich des Datenschutzrechts weitestgehend unbekannten Situation, für die es in Zukunft Empfehlungen und Best-Practice-Lösungen zu erarbeiten gilt, um Cybersicherheitsforschende und -forschungseinrichtungen ein hohes Maß an Rechtssicherheit für ihre Forschung zu geben und nicht nur durch, sondern auch während der aktiven Cyberabwehr die Grundrechte und -freiheiten der betroffenen Personen angemessen zu schützen.[39]

34 Vgl. Art. 1 DSGVO.

35 Bitkom e.V., 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen, Berlin, 2022, https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.

36 *Ebenda.*

37 *DSK*, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen, S. 2-3.

38 Vgl. ErwGr 85 DS-GVO; *DSK*, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen, S. 2-3.

39 *Selzer/Spiecker gen. Döhmann,* Rechtsrahmen der offensiven Cybersicherheitsforschung, Tagesspiegel, 2022, https://background.tagesspiegel.de/cybersecurity/warum-es-einen-rechtsrahmen-fuer-die-offensive-cybersicherheitsforschung-braucht.