AUSFALL IM STÖRFALL?
NETZKOMMUNIKATION IN KRISENSITUATIONEN

Zusammenfassung der Beiträge zur Veranstaltung „Ausfall im Störfall? Netzkommunikation in Krisensituationen" der Reihe „denkraum_medien" der Friedrich-Ebert-Stiftung / Medienpolitik am 16. April 2018 in Berlin. Referent_innen waren Dr. Aleksandra Sowa, Expertin für Informationssicherheit, Datenschutz und Buchautorin, Michael Bartsch, Geschäftsführer der Deutor Cyber Security Solutions GmbH, Thomas-Gabriel Rüdiger, Kriminologe am Institut für Polizeiwissenschaft und Vera Linß, Medienjournalistin und freie Moderatorin.

Das Internet ist global zum primären und konkurrenzlosen Kommunikationsnetz geworden. Als Ort für Teilhabe, Aktivismus und Selbstfindung haftete dem digitalen Raum zunächst der Ruf als Innovations- oder sogar als Revolutionskatalysator an. Mittlerweile hat die Cybereuphorie nachgelassen und Netzpessimismus verbreitet sich zunehmend, denn das Medium erweist sich als störanfällig und öffnet Tür und Tor für verschiedene Formen des Missbrauchs.

Die Liste ist lang, die Cybercrimevarianten zahlreich und doch gibt es bisher nur wenige Lösungsansätze: Wie soll man die Komplexität des Themas und der Kriminalitätsstrukturen überhaupt überblicken und was kann tatsächlich dagegen getan werden? FES Medienpolitik fasst die Ideen der drei geladenen Gäste zusammen und stellt deren Empfehlungen und Handlungsoptionen gegen Kriminalität im Cyberspace vor, um neue Impulse für sichere Kommunikation im Netz zu liefern.

KURZZUSAMMENFASSUNGEN DER DREI IMPULSVORTRÄGE

ALEKSANDRA SOWA

Aleksandra Sowa machte einleitend deutlich, dass das Internet, ursprünglich unter anderem vom US Department on Defense dazu erdacht, redundante Kommunikationswege gerade im Kriegs- oder Krisenfall zu gewährleisten, zum primären Kommunikationsweg evolviert ist.

Dessen Anfälligkeit für externe oder interne Angriffe stellt nicht nur die Sicherheit, sondern auch die zuverlässige Information der Bürger vor eine Herausforderung. Das Internet ist zum perfekten Medium der Desinformation geworden. Im Kontext von Wahlen bzw. Wahlkämpfen wurde das Problem bereits erkannt. Zum Verhängnis werde es jedoch tatsächlich dann, wenn die Zuverlässigkeit und Schnelligkeit der Infomation über Leben und Tod entscheiden kann – in Krisen oder Notfallsituationen, bei Sicherheitsvorfällen, Unfällen, Angriffen, Katastrophen, die die ganze Gesellschaft, Teile der Gesellschaft oder Gruppen von Individuen betreffen.

Die Versorgung der Bevölkerung mit Informationen in Krisen und Notfällen gehört zweifellos zu den wesentlichen gesellschaftlichen Bedürfnissen und staatlichen Verpflichtungen. Sie ist ein wesentlicher Bestandteil der Schutzpflicht des Staates seinen Bürgern gegenüber.

Sind der Staat, seine Institutionen, wie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), oder die Privatwirtschaft – die meisten kritischen Infrastrukturen befinden sich in Hand von Wirtschaftsunternehmen – für die Krisenkommunikation und zur Richtigstellung von Falschnachrichten verantwortlich? Was kann der Staat ohne die Hilfe der Privatunternehmen überhaupt noch leisten?

Mit dem IT-Sicherheitsgesetz und mit der Cyber-Sicherheitsstrategie des Innenministeriums hat die Bundesregierung die Unternehmen, die kritische Infrastrukturen betreiben, zur Einhaltung von IT-Sicherheitsmindeststandards nach dem Stand der Technik verpflichtet und ihnen bei wesentlichen Vorfällen Meldepflicht an das Bundesamt für Sicherheit in der Informationstechnik (BSI) bzw. an die Bundesnetzagentur (BNetzA) auferlegt, resümierte Aleksandra Sowa.

MICHAEL BARTSCH

Michael Bartsch sieht die Gesellschaft zum ersten Mal an dem Punkt, wo technologisch ein Wandel vorangetrieben werde, der nicht mehr zu stoppen sei. Dies bedeute, Technologien und neuen Geschäftsmodellen ausgeliefert zu sein.

Weil Bequemlichkeit und geringe Kosten im Mittelpunkt des Interesses der Nutzer stünden, komme der Sicherheit geringe Bedeutung zu. Das führe dazu, dass die Unternehmen ihre Geschäftsmodelle immer weiter digitalisieren, immer weiter automatisieren. Die Wertschöpfung findet heute, weltweit gesehen, zu weit über 60 Prozent durch digitale Medien, Computer und Vernetzung statt, so Bartsch. Die IT-Sicherheitsindustrie verweist auf ihre erfolgreichen Cyberstrategien,

daneben gibt es auf Cybercrime spezialisierte Polizeieinheiten. Aber die durchschnittliche Entdeckungszeit von Spionage- und Sabotage-Trojanern in Unternehmen ist von 220 auf ungefähr 450 Tage angestiegen. Weder auf Unternehmens- noch auf Staatsseite wisse man, wie das Problem in den Griff zu bekommen sei.

Weil die Anfälligkeit kritischer Infrastrukturen sofort ein politisches Problem darstellt, wird eilig nach Regelungen gesucht. Als Folge kaufen Unternehmen Sicherheitslösungen nach dem „Stand der Technik", wie gesetzlich gefordert. Aber der chinesische, russische oder sonstige Hacker findet die Lücke. Versagte die Technik? Hatte man den falschen Berater?

Den Angreifer, ob staatlich oder nicht staatlich, interessiere die Technologie nicht, er möchte den Geschäftsprozess stören. Der Automobilbauer, bei dem die Bänder von außen an und aus gemacht werden, wird bestimmt ein paar Millionen bezahlen, damit das Problem nicht wieder auftritt. Das sind heute die kriminellen Geschäftsmodelle, auf die wir uns vorbereiten müssen, prognostizierte Michael Bartsch.

THOMAS-GABRIEL RÜDIGER

Für Thomas-Gabriel Rüdiger sind soziale Medien wie WhatsApp, Facebook, Instagram, LinkedIn nicht nur Kommunikationsplattformen, sondern eine Art öffentlicher Raum - vergleichbar dem Straßenverkehr. Aber für den digitalen Raum, der keine physischen Grenzen kennt, wurde bislang kein einheitliches Normenverständnis entwickelt. Dennoch ist das Internet kein rechtsfreier Raum. Recht gilt überall.

Bei sexueller Belästigung oder Missbrauch von Kindern, Volksverhetzung im Internet, Beleidigungsdelikten, Sex-Erpressung – überall gebe es hohe Aufklärungsquoten. Das Problem bestehe allerdings darin, dass es nur ganz wenige Anzeigen gebe, aber große Dunkelfeldzahlen, problematisiert der Kriminologe. Täter müssten nur eine geringe Angst vor Strafverfolgung im Internet haben. Im Verhältnis zum physischen Raum sei der Strafverfolgungsdruck sei nicht hoch genug.

Die Strafverfolgung konzentriere sich häufig auf Hacking und große kritische Infrastrukturen. Auch könne davon ausgegangen werden, dass die Sicherheitsbehörden sich eher auf die Strafverfolgung im Darknet konzentrieren würden, als im Visual Web. Aber das Miteinander der Menschen in diesem Raum erhalte zu wenig Aufmerksamkeit. Es fehlten Antworten, wie man mit der Kriminalität, die daraus entsteht, eigentlich umgehen solle.

Es werde bisher beispielsweise zu wenig gefragt: Was mache ich, um Kinder im digitalen Raum zu schützen? Denn dieser digitale Raum sei davon geprägt, dass unbekannte Erwachsene ganz selbstverständlich in eine anonymisierte Interaktion mit Kindern und Jugendlichen treten können. Hierauf hat die Gesellschaft – sowohl die Politik, als auch die Betreiber – noch keine Antwort. Nach einer Studie von Jugendschutz.net, haben 99 von 100 Spiele-Apps gefährliche oder gefährdende Inhalte für Kinder und Jugendliche.

Aus Sicht von Thomas-Gabriel Rüdiger liegt die Aufgabe einer digitalen Polizeiarbeit nicht nur darin, kritische Infrastrukturen zu schützen, sondern es braucht auch eines Ansatzes, wie in der digitalen Welt die Kinder und Jugendlichen geschützt werden können.

Die Herausforderung besteht darin, eine Generation heranwachsen zu lassen, die es nicht als Selbstverständlichkeit begreift, sexuelle Übergriffe im Netz erleben zu müssen, und die es auch nicht als Selbstverständlichkeit begreift, auf Hatespeech zu treffen oder mit Cybermobbing konfrontiert zu werden.

Aus Sicht des Polizeiexperten ist eine Grundbedingung für ein besseres Miteinander im digitalen Raum, dass eine Straftat mit höherer Wahrscheinlichkeit geahndet wird.

ZUSAMMENFASSUNG DER PODIUMSDISKUSSION

Die drei Perspektiven aus den Bereichen Informationssicherheit und Datenschutz, Wirtschaft und Polizeiwissenschaft haben einige der Schwachstellen und Herausforderungen aufgezeigt, die bei der Nutzung des Internet als primären Kommunikationskanal verborgen liegen. Dringlicher denn je gilt es also potenzielle Lösungsansätze zu finden, um das Netz sicherer zu machen. Eine öffentliche Diskussion über neue Wege zur Bekämpfung der digitalen Wirtschaftskriminalität finde kaum statt und wenn, scheitere sie den Referent_innen zufolge vor allem an der Komplexität der Thematik, fehlenden Geschäftsmodellen und Konzepten, fehlendem Geld oder dem Unwillen, in Sicherheit zu investieren und schlussendlich an der Widersprüchlichkeit der digitalpolitischen Agenda der Regierung. Doch wie können konkrete nächste Schritte aussehen, die schon bald für mehr Sicherheit im Netz sorgen?

Die Moderatorin **Vera Linß** verdeutlicht die Auswirkungen der Cyberkriminalität:

2016 haben Cyberangriffe weltweit Schäden in Höhe von bis zu 450 Milliarden Dollar verursacht, davon 65 Milliarden Dollar bei Unternehmen in Deutschland. Die zwei größten Probleme in diesem Zusammenhang sieht sie im verbreiteten Gefühl von Kontrollverlust und zu geringem Wissen darüber in der Öffentlichkeit.

Aus Sicht von **Michael Bartsch** ist die Komplexität zu hoch. Gekauft werden heute Technologien, von denen die Experten zwar wissen, wie man sie benutzt, aber nicht mehr, wie sie funktionieren. Für das Beseitigen von Sicherheitslücken gibt es keinen Mechanismus. Ein defektes Auto wird zurückgerufen und repariert. Bei einem Computersystem geht das nicht.

Thomas-Gabriel Rüdiger sieht die Sicherheitsbehörden in der Pflicht. Es müsse ernsthaft hinterfragt werden, wie Sicherheit im digitalen Raum hergestellt werden kann. Viel zu wenig Beamte werden für den digitalen Raum eingesetzt. Nicht einmal ein Prozent des Personals der Sicherheitsbehörden wären für den digitalen Raum zuständig. Ein Beispiel: Die Bundeswehr hat vor einiger Zeit 71 Millionen Cyberangriffe auf die kritischen Infrastrukturen gezählt. Wenn davon nur zehn Prozent zur Anzeige bei der Polizei gekommen wären, dann wäre das mehr gewesen als die gesamte polizeiliche Kriminalstatistik von Mord bis Urheberrechtsverletzungen überhaupt aufweist.

Aleksandra Sowa stellte klar: Einen separaten Cyberspace, von dem die Politik spricht, gibt es in Wirklichkeit nicht. Alle Gesetze, die im ganz normalen täglichen Leben für Unternehmen und Privatpersonen gelten, gelten auch im Cyberspace: „Was offline gilt, gilt auch online". Aber es fehlen die Möglichkeiten der Kontrolle, man spricht oft, gerade im Kontext des Datenschutzes, vom „Vollzugsdefizit". Es gibt Gesetze, zum Beispiel das IT-Sicherheitsgesetz, die Datenschutzgrundverordnung, die Vorgaben machen. Aber jetzt müssten auch Wege gefunden werden, die Umsetzung zu prüfen, zu kontrollieren. Transparenz sei wichtig. Sie sei eine notwendige, aber nicht hinreichende Bedingung für die Prüfbarkeit.

Michael Bartsch setzte dieser Einschätzung seine eigene Sicht entgegen und bezweifelte die Wirksamkeit von gesetzlichen Regelungen. Dafür drehe sich die digitale Welt zu schnell. Da sei ein Gesetz nicht das richtige Mittel, langfristig dafür zu sorgen, dass die Sicherheit erhöht wird. Das heiße als allererstes: „Wie kann die Gesellschaft medienkompetent werden, damit sie das Internet gefahrenfrei nutzen kann?" Das habe etwas mit Bildung, mit Erziehung zu tun, mit Verantwortung.

Letztlich müsse Security aber auch Geschäftsmodell werden. Man müsse sich die Frage stellen: Was möchte ich an Sicherheit erreichen? Was bin ich bereit, dafür zu bezahlen?

Ob es in einer demokratischen Gesellschaft Privacy oder Security nur für diejenigen geben sollte, die es sich leisten können, ist für **Aleksandra Sowa** eine wichtige Frage. Oder sollte dafür gesorgt werden, jedem – auch im Sinne einer solidarischen Gesellschaft – den Zugang zu geschützten Geräten zu ermöglichen?

Das Bundesinnenministerium hat in der Cyber-Sicherheitsstrategie 2016 das erste Mal „Security by Design" als ein strategisches Ziel festgeschrieben, aber die Haftungsfrage noch weitgehend offen gelassen: Wer ist verantwortlich, wenn zum Beispiel das Betriebssystem oder die Software auf einem Handy, in einem Auto nicht sicher ist, angegriffen werden kann und dadurch ein Unfall passiert oder gar jemand zu Schaden kommt? Der Hersteller, der Nutzer oder der Provider? Die Haftungsfragen bleiben, trotz Konkretisierung im Koalitionsvertrag, noch weitgehend ungeklärt. Es gebe aber die Idee eines IT-Gütesiegels. Das heißt, man möchte Produkte – und insbesondere deren Software – kennzeichnen, und dem Nutzer damit sichtbare Qualitäts- und Sicherheitsmerkmale an die Hand geben.

Thomas-Gabriel Rüdiger hält eine Art sichtbare Polizeipräsenz im Netz für unerlässlich. Das habe wenig damit zu tun, ob ein Handy sicher sei. Das habe etwas damit zu tun, wie das alltägliche, öffentliche Miteinander im Netz im digitalen Raum funktioniert.

Der Kriminologe hält jedoch vor allem den Rechtsrahmen für reformbedürftig. So müsse die Polizei bedingt durch das Legalitätsprinzip bei jedem Delikt, bei jedem Anfangsverdacht, eine Strafanzeige aufnehmen. Ansonsten macht sie sich gegebenenfalls selbst strafbar. Aber im Netz sind die Delikte in einer so hohen Anzahl vorhanden, dass dies niemand bewerkstelligen kann. Die Sicherheitsbehörden könnten das Dunkelfeld selbst umfangreich aufhellen. Deswegen müsse der Rechtsrahmen eine Anpassung finden.

Der Kriminologe wies aber auch auf die Konsequenzen hin: Wenn die digitale Polizeiarbeit geändert würde, sei mit einer steigenden Kriminalitätsstatistik bei gleichzeitig sinkender Aufklärungsquote zu rechnen. Denn es ist wissenschaftlich belegt, dass mehr sichtbare Polizei zu mehr Anzeigen führt. Das heißt, wenn mehr Polizei im Netz zum Beispiel Sexualtäter effektiver bekämpfen soll, wird das dazu führen, dass hunderttausende von Delikten zur Anzeige gebracht werden. Das müsse die Gesellschaft aushalten.

FAZIT DER VERANSTALTUNG

Eine Steigerung der Sicherheit im digitalen Raum erfordert umfangreiche gesamtgesellschaftliche Neubewertung und Anpassungen der rechtlichen, wirtschaftlichen und ethischen Grundlagen und Konsequenzen. Es besteht daher dringender Bedarf, die Optionen offenzulegen, in einem transparenten, öffentlichen Diskussionsprozess zu analysieren und zu bewerten, um höchstmögliche Akzeptanz der erforderlichen politischen Entscheidungen zu erreichen. Dabei gilt es vor allem, den Schutz der bürgerlichen Freiheitsrechte zu wahren und das langsame Abgleiten in einen durch Zensur und Selbstzensur geprägten Überwachungsstaat zu verhindern. Der Staat, die Regierungen sollten wieder Technologien fördern, die neue Lebens- und Arbeitsentwürfe und sozialen Wandel ermöglichen, anstelle von Technik, die soziale Kontrolle verstärkt.

Einen Beitrag dazu wollen die entsprechenden Fachveranstaltungen der Friedrich-Ebert-Stiftung leisten.

Impressum

© 7/2018
Friedrich-Ebert-Stiftung
Herausgeberin: Politische Akademie/Medienpolitik
Godesberger Allee 149, 53175 Bonn
www.fes.de

Redaktion:
Peter Donaiski
Friedrich-Ebert-Stiftung
Politische Akademie/Medienpolitik
peter.donaiski@fes.de

ISBN: 978-3-96250-183-9