2010/25 Lifestyle

https://jungle.world/artikel/2010/25/angriff-auf-den-digitalen-untergrund

Über das europäische »Zentrum gegen Cyberkriminalität«

Angriff auf den digitalen Untergrund

Von **matthias monroy**

Das Internet gilt den Behörden der Europäischen Union als Tummelplatz von Terroristen und Verbrechern. Ein neues »Zentrum gegen Cyberkriminalität« soll Abhilfe schaffen.

Geht es nach dem Willen der EU-Innenminister, wird die Kontrolle des Internet bald auf eine neue Grundlage gestellt. Auf ihrer letzten Sitzung in Luxemburg hatten die Vertreter der Mitgliedsstaaten über neue Schritte zur Verfolgung von Internet-Kriminalität beraten. Der Kampf gegen »Kinderpornografie, sexuelle Gewalt, terroristische Aktivitäten, Angriffe auf elektronische Netzwerke, Betrug, Identitätsdiebstahl usw.« soll bald von einem »Zentrum gegen Cyberkriminalität« geführt werden, das vermutlich von der EU-Polizeiagentur Europol geleitet werden wird.
Eine gleichzeitig veröffentlichte Mitteilung der gegenwärtigen EU-Präsidentschaft, die von Spanien, Belgien und Ungarn gebildet wird, untermauert diese Pläne. Zunächst wird darin die Bedeutung des Internet als Informationsquelle, Marktplatz, Personalbeschaffungsstelle und Grundlage für das Geschäft mit Finanzdienstleistungen gepriesen. Kopfzerbrechen bereitet den Regierungen allerdings eine zunehmende Nutzung zur Informationsbeschaffung für allerlei »offline organisierte Kriminalität«, darunter Geldwäsche, Drogen- und Menschenhandel, Geld- und Produktfälschung sowie Waffenhandel.

Von den Behörden weitgehend unkontrolliert hat sich dem Bericht zufolge ein »digitaler Untergrund« gebildet, ein Handelsplatz für gestohlene Personen- und Finanzdaten. Als zusätzliche Risiken werden »Phishing, Pharming, Datenspionage, Malware Distribution und Hacking von Firmendatenbanken« genannt. Erneut gilt die Anonymität als Problem, da die Delinquenten zunehmend Verschlüsselungstechniken und Internet-Telefonie verwendeten, um Überwachung und Strafverfolgung zu erschweren. Zudem würden terroristische Gruppen das Netz für Propaganda, Radikalisierung, Rekrutierung oder gar als »virtuelles Trainingscamp« nutzen. Auch andere »extremistische Gruppen« seien mithilfe des Internet in der Lage, ihre zuvor lokal begrenzten Aktivitäten weltweit zu betreiben.
Die aktuelle deutsche polizeiliche Kriminalstatistik verzeichnet für 2009 steigende Fallzahlen bei der Cyberkriminalität, 206 909 Delikte wurden registriert. Während die zunehmende Netzkontrolle auf EU-Ebene häufig mit der Notwendigkeit begründet wird, gegen 1 500 Webseiten mit kinderpornografischem Inhalt vorgehen zu müssen, dokumentiert die deutsche

Statistik für dieses Delikt stark rückläufige Zahlen.
Die Bekämpfung der Kinderpornografie ist populär und soll repressive Maßnahmen rechtfertigen, ist aber nicht das einzige Motiv für den Wunsch nach einer stärkeren Kontrolle. Die ökonomische Bedeutung des Internet wächst, darauf verweist eine Mitteilung der EU-Kommission an das Europäische Parlament vom vergangenen Jahr. »Kritische Informationsinfrastrukturen«, zu denen das Internet gehört, werden dort als entscheidend für das wirtschaftliche Wachstum in der EU bezeichnet. Vor allem Unternehmen seien bezüglich Umsatz und Effizienz ihrer internen Abläufe auch vom Internet abhängig. »Kritische Informationsinfrastrukturen« werden für immerhin fast 40 Prozent des deutschen Produktivitätsanstiegs verantwortlich gemacht.
Der nun von der Europäischen Union entworfene Aktionsplan soll frühere Schlussfolgerungen und Initiativen zusammenfassen. Bereits bei der Verabschiedung der »Strategie zur Bekämpfung der Cyberkriminalität« hatte der EU-Ministerrat im Jahr 2008 eine härtere Gangart bei der Überwachung von Internetaktivitäten angedroht, die als Sanktion den Entzug ganzer Domains und IP-Adressen ermöglichen sollte. Neben gemeinsamen grenzüberschreitenden Internet-Streifen sieht das Repertoire auch »Ferndurchsuchungen« von Computern vor. Die deutsche Polizei könnte das hierzulande verharmlosend »Online-Durchsuchung« genannte Manipulieren von Rechnern fortan diskret über EU-Behörden ausführen.
So erscheint die Behauptung Jörg Zierckes, des Präsidenten des Bundeskriminalamts (BKA), dass sein Amt bislang keine »Online-Durchsuchung« durchgeführt habe, in einem anderen Licht. Das BKA ist für seine gute Zusammenarbeit mit Europol bekannt, Deutschland ist bislang Hauptzulieferer und auch größter Nutzer der Datenbanken von Europol. Während im vorigen Jahr 13,81 Prozent aller dort registrierten Fälle von deutschen Polizeibehörden eingereicht wurden, verzeichneten diese 20,35 Prozent aller Suchvorgänge.

Um moderne digitale Ermittlungsmethoden weiterzuentwickeln, wird im Papier über die »Strategie zur Bekämpfung der Cyberkriminalität« ein intensiver Informationsaustausch zwischen den Verfolgungsbehörden und dem »privaten Sektor« gefordert. Gemeint ist unter anderem der Software-Zweig der Sicherheitsindustrie, der für die Analyse der stetig wachsenden Datenmenge automatisierte Werkzeuge entwickelt. Zahlreiche Hersteller konkurrieren mit Plattformen zur Erschließung digitaler Information, die neben Textformaten auch Bild-, Video- und Audiodateien durchforsten können. Per »Data Mining« werden Zusammenhänge zwischen in Datenbanken oder dem Internet auffindbaren Personen und verdächtigen Objekten gesucht, die dann als »Risiko« klassifiziert und an Ermittler weitergereicht werden. Genutzt wird auch eine Software zur »Social Network Analyse« (SNA), die der Aufklärung von Beziehungen zwischen Personen, Sachen oder Objekten dient. Diese Art der Rasterfahndung hat nach Angaben von Europol bereits herausragende Erfolge erzielt. So sei es möglich, »Schlüsselpersonen« oder »versteckte Muster« in komplexen Datenmengen schnell sichtbar zu machen.
Ob die neue Internet-Überwachungszentrale innerhalb der EU-Polizeiagentur angesiedelt sein wird, ist zwar noch offen, aber wahrscheinlich. Sollte Europol den Zuschlag erhalten, ist die Bekämpfung des »islamistischen Terrorismus« wieder zum Wegbereiter für die Kontrolle abweichenden Verhaltens geworden. Unter Federführung der damaligen deutschen EU-Präsidentschaft hatte Europol bereits im Jahr 2007 die Initiative »Check the Web« gestartet, bei der die »Erforschung extremistischer islamistischer Internetseiten« von deutschen Behörden geleitet wird. Seit dem vorigen Jahr betreibt Europol zudem eine »Cyberkriminalität-Plattform«, auf der Polizeibehörden und Geheimdienste der EU gewonnene Daten sammeln, tauschen und analysieren.

Im Entwurf des neuen Cyberkriminalität-Aktionsplans werden die EU-Mitgliedsstaaten aufgerufen, ihre nationalen Systeme mit der Europol-Plattform kompatibel zu machen und mehr Daten auszutauschen. Prompt kündigte die kürzlich in Hamburg tagende Konferenz der Landesinnenminister (IMK) auch für Deutschland die Einrichtung einer »nationalen Internet-Zentralstelle« an. Gegenüber der Neuen Osnabrücker Zeitung beschwor der Hamburger IMK-Vorsitzende Christoph Ahlhaus (CDU) eine »rasant wachsende Bedrohung durch Kriminelle im Netz«, die mit einem »großen Wurf« aufgehalten werden müsse. Das Ziel sei ein umfangreiches Maßnahmenpaket, dessen »grundsätzliche Marschrichtung« eine Arbeitsgruppe definieren soll. Die »Internet-Zentralstelle« solle in jedem Fall Informationen von Bund und Ländern zusammenführen, verriet der Minister. Wie bei Europol ist die Einbeziehung von »Experten aus der Internet-Branche« geplant.

Ahlhaus äußert sich vorsorglich nicht über eine etwaige Kooperation oder Zusammenlegung mit dem 2007 gegründeten »Gemeinsamen Internetzentrum« (GIZ). Angesiedelt auf dem Gelände des »Gemeinsamen Terrorismusabwehrzentrums« in Berlin-Treptow sucht das Bundeskriminalamt zusammen mit Geheimdiensten nach »extremistischen und terroristischen Aktivitäten« im Internet. Der damalige Bundesinnenminister Wolfgang Schäuble hatte bei der Eröffnung des GIZ das Internet als digitale »Bibliothek des terroristischen Wissens« bezeichnet.

Nun hat sich mit Gilles Kerchové der Terrorismus-Koordinator der Europäischen Union in der Debatte um die Sicherheit des Internet zu Wort gemeldet. Er fordert, den Herausforderungen »Cyber-Terrorismus, Cyber-Kriminalität, Cyber-Attacken, Cyber-Krieg und Cyber-Sicherheit« mit einem »umfassenden Ansatz« zu begegnen. Kerchové kündigte einen baldigen Vorschlag hierzu an, nicht ohne auf die USA zu verweisen. Die US-Regierung hat im April ein neues militärisches Kommando zur Abwehr, aber auch Ausführung von Cyber-Angriffen eingerichtet.