Positionspapier Cybercrime

Straftaten im Bereich Cybercrime sind allgegenwärtig. Sowohl Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder andere Daten richten (Cybercrime im engeren Sinne) als auch die Verlagerung anderer Straftaten in das Internet (Taten werden mittels Informationstechnik begangen; Cybercrime als Tatmittel; auch als Cybercrime im erweiterten Sinne), passieren täglich.

Wenn die Politik bei der Bekämpfung von Cybercrime (beide Definitionen) glaubwürdig agieren will, muss sie der Kriminalpolizei und der Justiz das dafür notwendige zusätzliche Personal und die rechtlichen sowie technischen Instrumentarien zur Bewältigung dieser Aufgabe zur Verfügung stellen, aber auch für die erforderliche Qualifizierung Sorge tragen.

Zur Stärkung der Prävention sowie der repressiven Bekämpfung von Cybercrime fordert der BDK Anpassungen seitens des Gesetzgebers in folgenden Schwerpunkten:

Inhalt

Bund Deutscher Kriminalbeamter IT-Expertenkreis
Poststraße 4-5 | D-10178 Berlin
Tel.: +49 (0) 30.24 630 45 - 0 | Fax: +49 (0) 30.24 630 45 - 29
E-Mail: bdk.bgs@bdk.de | Internet: www.bdk.de

Personal

1. Einstellung von IT-Experten mit abgeschlossenen Studiengängen (z.B. in Informatik, Mathematik sowie Betriebswirtschaftslehre) und / oder Fortbildung zum Kriminalisten.

2. Die Besoldung sollte zwischen A 12 und A 14 bzw. den entsprechenden Entgeltgruppen liegen, um gegenüber der freien Wirtschaft an Attraktivität zu gewinnen.

3. Die Verbeamtung von Tarifbeschäftigten sollte das grundsätzliche Ziel zur langfristigen Bindung der Beschäftigten sein.

Qualifikation / Aus- und Fortbildung

1. Jeder Polizeibeamte muss durch seine Ausbildung in die Lage versetzt werden, einfache Cybercrimedelikte im Bereich der Alltagskriminalität (Verlagerung von Straftaten in das Internet bzw. Nutzung des Internet als Tatmittel) selbst zu bearbeiten. Zusätzlich ist die Einrichtung von leistungsfähigen Spezialdienststellen zur Bekämpfung von Cybercrime im engeren Sinne in jeder Polizeibehörde erforderlich. Dies fördert zudem den Knowhow- und Informationsaustausch.

2. Bereits in den Aus- und Fortbildungseinrichtungen der Bundes- und Länderpolizeien muss ein starker Fokus auf IT-Aspekte gelegt werden. Zudem müssen adäquate weiterführende Aus- und Fortbildungsmaßnahmen angeboten und allen Bedarfsträgern sowie Interessierten zugänglich gemacht werden. Bei der Planung und Durchführung von Fortbildungen sollten über behördeneigene Veranstaltungen auch Online-Seminare sowie Weiterbildungsmöglichkeiten externer Dienstleister berücksichtigt werden.

Optimierung der Arbeitsabläufe

1. Ressourcenorientierte Prozessoptimierung bei der Bearbeitung von Cybercrime-Massendelikten in Abstimmung mit der Staatsanwaltschaft, z.B. bei der Bearbeitung von KiPo-Hinweisen. Aufgrund fehlender Verkehrsdatenspeicherung können meist keine Rückschlüsse mehr auf den Nutzer der im Hinweis gemeldeten IP Adresse gezogen werden.

2. Zeitnahe Implementierung aktueller internationaler Standards für IT-Forensik.

3. Benennung von Schwerpunktstaatsanwaltschaften mit ausschließlicher Zuständigkeit für Cybercrime-Delikte; zentrale Ermittlungsführung bei Staatsanwaltschaften für bestimmte Phänomenbereiche.

4. Kriminalistische Aus- und Fortbildung für Richter und Staatsanwälte, gemeinsam mit Cybercrime-Ermittlern.

5. Bildung von Bund-Länder-Ermittlungsgruppen zur zeitnahen und gemeinsamen Bearbeitung großer Verfahren, z.B. Ransomware-Wellen. Die Zuständigkeit dafür muss bei einer Schwerpunktstaatsanwaltschaft liegen.

6. Die KRITIS-Meldeverpflichtungen gemäß IT-SicherheitsgesetzG sind zu überprüfen. Andere, derzeit noch nicht zur Anzeige verpflichtete Firmen, sollten zur freiwilligen Meldung motiviert werden; Einführung und Durchsetzung von Sanktionen bei Verstößen gegen die Meldepflichten nach dem Informationssicherheitsgesetz.

7. Unmittelbare polizeiliche und justizielle Rechtshilfe in Europa, Reform der Rechtshilfe, Anspruch auf Sofortauskunft innerhalb 24 Stunden, sofortige Sicherung von Beweismitteln bei nachfolgendem Rechtshilfeersuchen.

PKS

Einführung einer Gruppe Cybercrime in der PKS

Hierin sollen alle dem Phänomen Cybercrime (im engeren Sinne) zuzuordnenden Delikte zusammengefasst werden. Bisher finden sie sich verteilt in diversen Gruppen.

1. Im Deliktsfeld Cybercrime muss von einem sehr hohen Dunkelfeld ausgegangen werden. Bisher wird Cybercrime in der PKS nur zu geringen Teilen erfasst (Voraussetzung ist seit 2014, dass Anhaltspunkte für einen Tatort in Deutschland vorliegen), was die Erstellung eines realistischen Lagebildes unmöglich macht.

2. Eine Vielzahl krimineller Handlungen im Internet wird aufgrund immer besserer technischer Sicherungen von den Betroffenen meist nicht bemerkt (lediglich Versuchsstadium). Eine Anzeige (und somit Erfassung) erfolgt folglich nicht.

3. Angriffswellen der digitalen Erpressung (Ransomware) werden in der PKS trotz einer Vielzahl von Opfern (z.B. bei 1,2 Mio. bei Angriffen auf die Router der Deutschen Telekom) nur als 1 Fall von Computersabotage (Cybercrime im engeren Sinne) erfasst.

Rechtsforderungen

TKG / TMG:

Definition und Durchsetzung internationaler Standards bei Providern in Bezug auf die zu erhebenden Telekommunikationsdaten und deren Übermittlung an die Strafverfolgungsbehörden: im Telekommunikations- und Telemediengesetz sind umfassende Reformen notwendig, um eine effektive Zuordnung von Rufnummern / Anschlüssen zu Personen zu ermöglichen.

1. Gleichstellung von Telemedien- und Telekommunikations-Dienstleistern im Hinblick auf die Verpflichtungen zur Speicherung, Herausgabe von Bestandsdaten, Verkehrs- sowie Nutzungsdaten.

2. Telemedien- und Telekommunikations-Dienstleister sollten zur Mitwirkung, z.B. in Form der Umsetzung einer richterlichen Überwachungsanordnung, verpflichtet werden.

3. Verpflichtung zur Einrichtung einer 24/7 Erreichbarkeit von Providern sowie Festlegung von Antwortfristen in TKG und TMG.

4. Mobilfunkbetreiber sollten zur Speicherung der zur Identifizierung des konkreten Nutzers benötigten Daten – speziell die „öffentliche IP-Adresse“ sowie die Portkennung, verpflichtet werden. Da die IP-Adresse in vielen Fällen das einzige Identifizierungskriterium darstellt, ist zu prüfen, in wie weit die gesetzliche Speicherfrist von 10 Wochen den polizeilichen Bedarfen entspricht, oder ob die Frist ausgeweitet werden sollte.

Verkehrsdatenspeicherung:

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten ist nach einer Übergangsfrist am 01.07.2017 offiziell in Kraft getreten. Aufgrund der weiterhin ausstehenden Entscheidung zur Vereinbarkeit des Gesetzes mit geltendem EU-Recht teilte die Bundesnetzagentur (BNetzA) daraufhin öffentlich mit, dass bis zu einer rechtskräftigen Entscheidung keine Anordnungen oder sonstige Maßnahmen zur Durchsetzung der Speicherverpflichtung gegenüber TK-Unternehmen erfolgen würden. Das hatte zur Folge, dass kein Unternehmen in Deutschland die Verkehrsdatenspeicherung umsetzte und damit für die Gefahrenabwehr und Strafverfolgung dringend benötigten Daten weiterhin nicht zur Verfügung stehen. Es muss auf eine vollständige und lückenlose Umsetzung der Mindestspeicherfristen hingewirkt werden.

1. Die Wirkung der Rechtsprechung des OVG Münster muss klargestellt werden. Lediglich das BVerfG verfügt über eine Verwerfungskompetenz für nationale Regelungen verfügt. Das OVG Münster hat am 22.06.2017 entschieden, dass ein einzelner Internetdienstanbieter bis zum Abschluss des Hauptverfahrens einstweilen von der Speicherpflicht befreit ist. Der Beschluss des OVG Münster hat auf die Gültigkeit der Normen zur Speicherpflicht für die sog. Vorratsdaten jedoch keinen Einfluss – **diese gelten unstreitig seit dem 01.07.2017 für alle anderen TK-Anbieter**. Denn die Nichtigkeit gesetzlicher Normen kann nur das Bundesverfassungsgericht bestimmen.

2. Bei Straftaten im und über das Internet ist die Zuordnung einer dynamisch vergebenen IP-Adresse zu einem bestimmten Anschluss in Deutschland oftmals einziger Anknüpfungspunkt der Strafverfolgung und demnach die einzige Möglichkeit, einen konkreten Tatverdächtigen zu ermitteln. Solche Daten, die nur bei Internetservice-Providern vorhanden sind, können nur zur Ermittlung abgerufen werden, wenn diese sowieso vorhandenen (zu Abrechnungszwecken) Daten auch über einen längeren Zeitraum gespeichert werden. Aktuell ist der Erfolg eines Auskunftsersuchens „Glückssache“.

StPO / StGB:

Für die Ermittlung in Cybercrimedelikten werden derzeit überwiegend Hilfskonstruktionen im Rahmen der StPO angewandt, um notwendige Maßnahmen durchführen zu können. Teilweise muss deshalb auf erforderliche Maßnahmen verzichtet werden. Die Eingriffsnormen der Strafprozessordnung müssen mit Blick auf Cybercrime, besonders im Zusammenhang auf die Herausforderungen durch kryptierte Kommunikation (rechtliche Voraussetzungen für Quellen-TKÜ und Online-Durchsuchung anpassen bzw. klarstellen), reformiert werden.

1. Aufnahme von gewerbs- und bandenmäßiger Begehungsformen der Straftaten im Bereich Cybercrime im engeren Sinnen in den Katalog gem. §100a StPO.
2. Einsatz der Online-Durchsuchung zu Zwecken der Strafverfolgung (in herausragenden Fällen, z.B. Kriterienkatalog gem. §100a StPO)
3. Befugnis zur Erhebung von Verkehrsdaten nach §113b TKG zur Gefahrenabwehr
4. Ergänzung einer speziellen und damit klarstellenden Befugnis zur Erhebung von Bestandsdaten der Telemediendienstleister nach §14 TMG (einschließlich Log-in-IP, derzeit noch §15 TMG)
5. Verpflichtung der Provider, aktiv die Einschränkungen des Internetzugangs infizierter Rechner auf ausgewählten Websites zu betreiben (wallet gardens)
6. gesetzliche Verpflichtung der Internet-Service-Provider zu Legitimationsprüfungen von Kundendaten, z.B. Freemailer, Anmietung von Serversystemen, zur Verhinderung der anonymen Nutzung des Internet (analog hierzu auch die Verpflichtung für Betreiber von Hotspots und Internet-Cafés).
7. Schaffung eines Straftatbestands des Betreibens illegaler Handelsplattformen und Foren
8. Umsetzung der Regelungen des Art. 16, 29 CoC zu Preservation Order (Vorabsicherung)
9. Übernahme von digitalen Identitäten für Ermittler im Darknet / Internet

BKAG:

1. Originäre Gefahrenabwehrzuständigkeiten i.S. Cybercrime für das BKA
2. Befugnis zur Erhebung von Verkehrsdaten nach §113b TKG zur Gefahrenabwehr
3. Ergänzung der Regelungen zur Quellen-TKÜ und Online Durchsuchungen zum Zweck der Gefahrenabwehr nach §4a BKAG

Prävention

1. Verstärkung der Präventionsarbeit zur Verhütung von Cybercrime: Nur durch zeitnahe Analyse von entsprechenden Phänomen und immer wieder angepassten Präventionstipps kann eine effektive Präventionsarbeit erfolgen. Verbraucherschutzzentralen sind in die Präventionsarbeit einzubinden. Rechtliche Stärkung des Verbraucherschutzes im Netz, gegen Abo-Fallen, kriminelle Callcenter, Spams, Ransomware usw. Gemäß einer aktuellen Bitkom Umfrage sind bereits 47% der Internet-Nutzer im letzten Jahr Opfer von Cybercrime geworden, fast jeder Zweite erlitt dabei einen finanziellen Schaden.

2. Anwendungssoftware im Bereich mobiler Betriebssysteme (Apps) bieten Einfallstore für Kriminelle, um auf Daten von mobilen Endgeräten zuzugreifen. Es muss deutlich gemacht werden, dass solche mobile Endgeräte de facto Computer sind und man auch in gleichem Umfang darauf zugreifen kann.