Im Einsatz – im Thema.
POLIZEI PRAXIS

CYBERCRIME - EINE AKTUELLE ANALYSE DEUTSCHER SICHERHEITSBEHÖRDEN

Der am 4.1.2019 bekannt gewordene Datendiebstahl, der zahlreiche Politiker und Prominente betraf – veröffentlicht wurden Handynummern, Mail- und Privatadressen, Kontoauszüge, Chatverläufe sowie Privatfotos –, dominierte die mediale Berichterstattung für einige Zeit.[1] Cyberkriminalität ist ein weltweites Phänomen, das weder an Landesgrenzen noch vor verschlossenen Türen Halt macht. Cybercrime kann überall stattfinden, wo Menschen Computer, Smartphones und andere IT-Geräte benutzen, in Firmen, Behörden, Universitäten, zu Hause und unterwegs.[2]

Die Polizeiliche Kriminalstatistik zeigt zwar seit Jahren steigende Fallzahlen im Bereich Cybercrime auf, spiegelt die aufgeführten Untersuchungsergebnisse im Bereich Cybercrime allerdings nicht annähernd wider. Daher muss bei der polizeilichen Betrachtung von Cybercrime von einem sehr großen Dunkelfeld ausgegangen werden, sprich: Vermutlich wird nur ein kleiner Teil der Straftaten in diesem Bereich zur Anzeige gebracht bzw. ist der Polizei und/oder den Strafverfolgungsbehörden bekannt.[3]

Nach Angaben des Bundeskriminalamtes umfasst Cybercrime die Bandbreite illegaler Aktivitäten und Tatgelegenheiten im bzw. mittels des Internets, die von der Verbreitung von Kinderpornografie im Internet über „Phishing“ persönlicher Zugangsdaten, Handel mit Waffen und Rauschgift bis hin zu Netzwerkeinbrüchen und DDoS-Attacken, der Verbreitung von Schadsoftware und Betrugshandlungen reicht.[4]

Cybercrime nutzt sowohl das Clearnet/Visible als auch das DeepWeb und Darknet. Im Phänomenbereich Cybercrime ist stellen die deutschen Sicherheitsbehörden in den letzten Monaten eine massiv steigende Kriminalitätsentwicklung fest.

Cyber-Angriffe können sich gegen Privatpersonen – oftmals deren Smartphone – richten, aber auch gegen große Unternehmen. Hacker verschaffen sich häufig Zugang zu Firmennetzwerken, indem sie mit zielgerichteten Spear-Phishing-Mails Mitarbeiter dazu bewegen, auf verseuchte Anhänge oder Links zu klicken.[5] Hierbei ist von einer hohen Dunkelziffer für Cyberangriffe auszugehen, da betroffene Firmen aus Angst vor Reputationsverlusten nicht immer Anzeige bei der Polizei erstatten.

Das Bundeskriminalamt definiert Cybercrime wie folgt:

Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.[6]

Die aktuell verbreiteten Erscheinungsformen von Cybercrime sind geprägt von einer Infektion und Manipulation von Computersystemen mit Schadsoftware, beispielsweise um

· persönliche Daten und Zugangsberechtigungen des Nutzers abgreifen und missbräuchlich nutzen zu können (Identitätsdiebstahl)
· darauf befindliche Daten/Dateien des Nutzers mittels sog. Ransomware zu verschlüsseln, um "Lösegeld" zu erpressen
· sie „fernsteuern“ zu können, in sog. Botnetzen zusammenzuschalten und für weitere kriminelle Handlungen einzusetzen.[7]

Zuständige Behörden und ihre Aufgaben

Für den Phänomenbereich IT-Sicherheit und Cybercrime zuständige Behörden in Deutschland sind:

· das Bundesamt für Sicherheit in der Informationstechnik (BSI)
o Cyber-Sicherheit und Kritische Infrastrukturen
o Beratung für Staat, Wirtschaft und Gesellschaft
o Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung
o Krypto-Technologie und IT-Management für erhöhten Sicherheitsbedarf[8]

· die Polizeien
o Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft[9]
o Für die Strafverfolgung und Bekämpfung von Cyberkriminalität sind in Deutschland zunächst die Landeskriminalämter und auf Bundesebene das Bundeskriminalamt zuständig. Hierbei nimmt das BKA eine koordinierende Funktion als Zentralstelle wahr und veröffentlicht jedes Jahr das Bundeslagebild Cybercrime[10]

· das Cyber-Abwehrzentrum (unter Federführung des BSI arbeiten hier das Bundeskriminalamt, die Bundespolizei, die Nachrichtendienste und die Bundeswehr zusammen)

o Das Cyber-Abwehrzentrum soll die operative Zusammenarbeit optimieren und Schutz- und Abwehrmaßnahmen koordinieren. Dies geschieht auf Basis eines ganzheitlichen Ansatzes, der die verschiedenen Gefährdungen im Cyberraum zusammenführt: Cyber-Spionage, Cyber-Ausspähung, Cyber-Terrorismus und Cyber-Crime. Das Ziel ist ein schneller Informationsaustausch, schnelle Bewertungen und daraus abgeleitete konkrete Handlungsempfehlungen
o Im Cyber-Abwehrzentrum werden alle Informationen zu Cyber-Angriffen auf Informationsinfrastrukturen zusammengeführt, von denen die sicherheitsrelevanten Behörden erfahren. Sie tauschen dort ihre Erkenntnisse aus und bewerten sie. Jede Behörde aus ihrer Sicht und in ihrer Zuständigkeit. So sollen alle Behörden in ihrem jeweiligen Zuständigkeitsbereich von dem gemeinsamen Wissen profitieren[11]

· das Bundesamt für Verfassungsschutz (BfV)

o Zur Erhöhung der Cybersicherheit gibt das BfV aus seinem Erkenntnisaufkommen stammende Hinweise auf bestimmte IT-Infrastrukturen, die für Cyberangriffe genutzt werden. Mit diesen Informationen werden gefährdete Stellen in die Lage versetzt eine eigene Betroffenheit festzustellen, potentielle Zugriffe von diesen Infrastrukturen auf ihr IT-Netzwerk im Vorfeld zu sperren und so den Schutz gegen Cyberangriffe zu erhöhen.[12]

· der Bundesnachrichtendienst (BND)

· das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr

o stellt mit einem Gemeinsamen Lagezentrum ein fusioniertes Lagebild des Cyber- und Informationsraums für die Bundeswehr und weitere Ressorts zur Verfügung
o koordiniert als Kommandobehörde die bundeswehrgemeinsame Erfüllung für die Erbringungsdimension Cyber- und Informationsraum aus dem Aufgabenspektrum der Bundeswehr, die im Frieden sowie im Spannungs- und/oder Verteidigungsfall in nationaler Verantwortung wahrgenommen werden[13]

Das aktuelle Bundeslagebild Cybercrime des Bundeskriminalamtes

Beim jährlichen Bundeslagebuld des BKA muss angemerkt werden, dass sich das Bundeslagebild Cybercrime auf

die im Hellfeld erfassten Straftaten beschränkt. Das Bundeskriminalamt selbst geht davon aus, dass das Dunkelfeld wesentlich mehr Straftaten im Bereich Cybercrime aufweist.[14] Nach Analyse des Bundeskriminalamtes stiegen die Fallzahlen im Bereich Cybercrime im Jahr 2017 an, Schätzungen zum Dunkelfeld und aktuelle Forschungsergebnisse unterstreichen das hohe Gefährdungs- und Schadenspotenzial von Cybercrime.[15]

Dabei steigert die zunehmende Bedeutung der IT für Unternehmen, Behörden und für den privaten Bereich die Manipulations- und Angriffsmöglichkeiten und aktuelle Technologietrends eröffnen neue Tatgelegenheiten und werden die Bedrohungslage weiter verschärfen. Zudem deuten polizeiliche Ermittlungsergebnisse darauf hin, dass sich die Täter im Bereich Cybercrime zunehmend professionalisieren, indem sie flexibel auf aktuelle technische Rahmenbedingungen reagieren. So begehen Cybercrime-Täter heute nicht mehr ausschließlich Straftaten im digitalen Raum, sondern bieten auch die zur Begehung von Straftaten erforderliche Schadsoftware oder komplette technische Infrastrukturen in der im Internet bestehenden kriminellen Schattenwirtschaft an.

Entsprechend eröffnen diese Werkzeuge aufgrund ihrer einfachen Handhabung auch Tätern ohne fundierte IT-Spezialkenntnisse die Möglichkeit, Straftaten mittels des Internets zu begehen.[16]

Daher werden zunehmend auch Kriminelle ohne spezifische Fachkenntnisse in die Lage versetzt, sich das für eine Tatbegehung erforderliche Know-how anzueignen und entsprechende Tools käuflich zu erwerben. Entsprechend weitete sich das Spektrum potenzieller Täter aus, weswegen generell eine steigende Quantität und Qualität von Cyber-Angriffen zu erwarten ist. Die vermeintliche Anonymität, die das Darknet jedem Nutzer bieten kann, macht diesen Bereich des Internets für Kriminelle besonders attraktiv, was auch für Gruppierungen der Organisierten Kriminalität gilt.

Im Allgemeinen kann ein arbeitsteiliges Zusammenwirken von Cyber-Kriminellen bei der Tatbegehung festgestellt werden. Nach Ansicht der Polizeibehörden sollte daher für eine erfolgreiche Bekämpfung von Cybercrime der Aspekt einer möglichen organisierten Tatbegehung im Fokus der Strafverfolgungsbehörden stehen.[17]

---

[1] Vgl. u.a. www.zeit.de/digital/datenschutz/2019-01/datendiebstahl-hackerangriff-politiker-faq; www.tagesschau.de/inland/hackerangriff-politiker-reaktionen-103.html; www.dw.com/de/datenklau-im-bundestag-hacker-angriff-auf-politiker/av-46964116; 27.1.2019.
[2] https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html; 27.1.2019.
[3]www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html; 27.1.2019.
[4]www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html; 27.1.2019.
[5] http://www.manager-magazin.de/digitales/it/bka-stellt-bundeslagebild-cybercrime-vor-a-1230442.html; 27.1.2019.
[6] Ebd.
[7]www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html; 27.1.2019.
[8] https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html; 27.1.2019.
[9] https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html; 27.1.2019.
[10] https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html; 27.1.2019.
[11] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html; 27.1.2019.
[12] https://www.verfassungsschutz.de/de/arbeitsfelder/af-cyberangriffe; 27.1.2019.
[13] Kommando Cyber- und Informationsraum (2019): Über uns.
[14] Bundeskriminalamt (2018): Bundeslagebild Cybercrime, S. 3.
[15] Ebd., S. 36.
[16] Ebd.
[17] Ebd.

Text: Dr. Stefan Goertz, Bundespolizei, Hochschule des Bundes, Lübeck, Bild: Gerd Altmann auf Pixabay

Alle Artikel dieser Kategorie