DPT

Deutscher Präventionstag –
der Jahreskongress seit 1995

Cybercrime – Strategien der Kriminalprävention

Eva Kühne-Hörmann

Aus: Erich Marks & Wiebke Steffen (Hrsg.):
Prävention und Freiheit. Zur Notwendigkeit eines Ethik-Diskurses
Ausgewählte Beiträge des 21. Deutschen Präventionstages
6. und 7. Juni 2016 in Magdeburg
Forum Verlag Godesberg GmbH 2017, Seite 391-396

978-3-942865-71-5 (Printausgabe)
978-3-942865-72-2 (eBook)

Staatsministerin Eva Kühne-Hörmann, MdL

„Cybercrime – Strategien der Kriminalprävention“

Das Medium Internet hat in den letzten Jahren und Jahrzehnten die persönlichen, gesellschaftlichen, wirtschaftlichen und auch politischen Entfaltungsmöglichkeiten signifikant erweitert. Die heutige Informationstechnologie zeichnet sich durch ihre Fähigkeit zur Integration in praktisch alle Bereiche des menschlichen Lebens aus und treibt damit die Digitalisierung unserer Welt voran. Über 92% der Berufstätigen und 100% der 14-19jährigen in Deutschland sind online. 99% der jungen Menschen im Alter zwischen 12 und 25 Jahren verbringen durchschnittlich über 18 Stunden wöchentlich im Internet.

Vor allem mobile Endgeräte und Alltagsapplikationen stehen dabei gegenwärtig im Vordergrund. Gerade die Nutzung sozialer Netzwerke ist - nicht nur für junge Menschen – eine Möglichkeit, weltweit und in Echtzeit zu kommunizieren, Bilder und Erinnerungen zu teilen sowie die eigene Persönlichkeit anderen vorzustellen.

Doch die enormen Entfaltungsmöglichkeiten, die das Internet bietet, dürfen nicht verdecken, dass es auch für Straftäter nahezu unbegrenzte Möglichkeiten bereithält, Straftaten in vorher nicht gekannter Weise zu begehen. Je umfassender sich die Gesellschaft in der digitalen Welt bewegt, desto mehr Tatgelegenheiten ergeben sich für Cyberkriminelle.

Zunächst ist festzuhalten, dass jeder – nicht nur die Internetnutzer – Opfer von Cybercrime werden kann, sei es der einzelne Bürger, Unternehmen oder auch staatliche Stellen. Mit der Zunahme der Bedeutung der IT als Bestandteil des Alltags der Bürger steigen die Manipulations- und Angriffsmöglichkeiten auf Seiten der Cyberkriminellen. Cyberkriminelle handeln global, nationale Grenzen spielen keine Rolle, wobei Handlungs-, Taterfolgs- und Aufenthaltsorte von Tätern und Opfern irrelevant sind. Das Internet bringt alles und alle zusammen. Bucht ein Bürger in Frankfurt am Main eine Urlaubsreise über Internet, hat der am anderen Ende der Welt wartende Straftäter in Echtzeit potentiellen Zugriff auf den für die Buchung genutzten Computer.

Aber auch diejenigen, die ihre Urlaubsreise nicht selbst über Internet buchen, können Opfer von Cybercrime werden, z.B. dadurch, dass die Täter sich Zugriff auf die persönlichen Daten durch einen Angriff auf die Server des Reisevermittlers verschaffen.

Das bedeutet kurz gefasst, dass durch das Internet erstmals in der Geschichte der Kriminalität Straftaten weltweit und unter Überwindung jeder räumlichen Distanz zwischen Täter und Opfer in Echtzeit begangen werden können.

Während dabei in der Vergangenheit meist eine relativ klare Zweiteilung der Cybercrime-Phänomene in technikbezogene Delikte – Cybercrime im engeren Sinne, etwa Ausspähen von Daten - und dem Internet als Tatmittel für allgemeine Straftaten wie etwa Betrug – Cybercrime im weiteren Sinne – beobachtet werden konnte, zeigt sich aktuell ein Trend zu kombinierten Angriffen auf Mensch und Maschine.

Die zunehmende technische Absicherung der Banken gegen Online-Banking-Betrug zum Nachteil von Bankkunden führt dazu, dass derzeit der Einsatz von Erpressungssoftware – Ransomware – für die Täter deutlich lukrativer ist. Krankenhäuser und andere Institutionen, aber auch Privatpersonen waren von diesen Vorfällen betroffen. Derartige Schadprogramme verschlüsseln Daten auf den Rechnern der Opfer sowie möglicherweise weiteren angeschlossenen Laufwerken und verlangen zur Wiederherstellung die Zahlung eines Lösegelds. Es handelt sich also um eine Form digitaler Erpressung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet täglich kurzzeitige, massive Spam-Wellen, deren E-Mail-Anhänge sog. Downloader beinhalten. Diese z.B. als Word-Dokumente oder JavaScript getarnten Dateien laden nach dem Öffnen unbemerkt Schadprogramme, wie die oben beschriebene Ransomware, nach. Haben die Opfer kein Backup ihrer Daten, bleibt nur noch die Wahl zwischen Zahlung des Lösegeldes oder dem Verlust der Daten.

Ein weiterer aktueller Trend ist die digitale Identitätsfälschung, bekannt unter dem Stichwort „Fake President Fraud“: Auf sehr überzeugende Weise ordnet mithilfe von Stimmenrekorder, E-Mail-Manipulation oder Ausnutzung ausspionierter Unternehmensabläufe ein fingierter Geschäftsführer einem Mitarbeiter persönlich eine Überweisung an. Die Betrugsopfer sind häufig größere, vor allem international arbeitende Firmen. Auch bei diesem Phänomen werden also technische Manipulationen mit Social engineering, also dem Einwirken auf Mitarbeiter, verbunden.

Diese beiden aktuellen Beispiele zeigen, dass erfolgversprechende Ansätze und Wege für Kriminalprävention im Cyberbereich immer auf beide Schwachstellen – Mensch und Technik – abzielen müssen. Demzufolge kann die Vorbeugung von Internetstraftaten mittels verbesserter technischer Maßnahmen erreicht werden, aber auch ganz herkömmlich durch Aufklärung und der Schaffung von Gefahrenbewusstsein. Neben technischen Maßnahmen wie der Verwendung von aktuellen Betriebssystemen, Browserplugins, Antivirensoftware und sicherer Passwörter sowie dem regelmäßigen Anlegen von Backups wichtiger Dateien heißt das: keine E-Mails unbekannter Absender öffnen, keine Daten preisgeben.

Gerade Unternehmen sind auf die Sicherstellung vertraulicher Daten angewiesen. Hierzu zählen meist bestimmte Personal- und Kundendaten, Finanzdaten oder auch Geschäftsgeheimnisse. Insbesondere in Unternehmen liegt das größte Problem regelmäßig nicht im fehlenden Sicherheitssystem der Rechner, sondern meist in der unzureichenden Sensibilisierung der Mitarbeiter. So sollten diese dahingehend geschult werden, welche Daten kommuniziert werden können und welche nicht.

Auch um das Risiko einer Infektion mit Schadsoftware im Vorhinein zu minimieren, empfiehlt sich die regelmäßige Schulung von Mitarbeitern. Insbesondere Abteilungen, in denen häufig E-Mail-Anhänge von unbekannten Absendern geöffnet werden – z. B. in Personalabteilungen eingehende Bewerbungen – gelten als besonders exponiert. Aber auch beim Öffnen von E-Mails vermeintlich bekannter Verfasser sollte stets auf Unregelmäßigkeiten geachtet werden, schließlich könnte sich ein Angreifer z. B. Zugriff auf das Postfach des Absenders verschafft haben. Sind die Mitarbeiter in der Lage, bösartige E-Mails vor dem Öffnen zu erkennen, bedeutet dies einen signifikanten Sicherheitsgewinn für die Unternehmens-IT.

Neben Unternehmen, die in großem Umfang auf die Nutzung des Internets angewiesen und damit besonders verwundbar sind, spielt Prävention bei Cyberdelikten in einem völlig anderen Bereich eine herausragende Rolle. Ich meine damit den Schutz von kindlichen und jugendlichen Internetnutzern vor digitaler Gewalt. Cybermobbing, Cyberstalking und Cybergrooming kann mit technischen Präventionsmaßnahmen kaum wirksam vorgebeugt werden. Der Schutz der Betroffenen und ihre ausreichende Sensibilisierung für die Gefahren kann primär durch Aufklärung und Schaffung von Medienkompetenz verbessert werden. In diesem Sinne kümmert sich der Landespräventionsrat in Hessen bereits seit Längerem um die Problematik „Cybermobbing“.

Zudem hat es sich bewährt, operativ tätige Staatsanwältinnen und Staatsanwälte an interdisziplinär besetzten Präventionsveranstaltungen gemeinsam mit Polizeibeamten, Pädagogen und Kinder- und Jugendpsychologen teilnehmen zu lassen. Erfahrene Strafverfolger kennen die Phänomene der Internetkriminalität unmittelbar und können ihre Erfahrungen häufig besonders eindrücklich vermitteln.

Mit der Zentralstelle zur Bekämpfung der Internetkriminalität (kurz ZIT) besitzt Hessen seit dem Jahr 2010 eine spezialisierte Ermittlungseinheit für diesen Kriminalitätsbereich. Die ZIT bearbeitet hessenweit Ermittlungsverfahren wegen besonders schwerwiegender oder umfangreicher Internetstraftaten und arbeitet dabei eng mit dem Bundeskriminalamt und dem Hessischen Landeskriminalamt zusammen. Im Jahre 2011 hat die ZIT durch intensive Ermittlungen dafür gesorgt, dass die bundesweit bekannte Plattform für Cybermobbing namens „Isharegossip“ von den Tätern aus dem Netz genommen wurde, um dem Verfolgungsdruck zu entgehen. Die fehlende Vorratsdatenspeicherung verhinderte damals die Identifizierung und Ergreifung der Täter.

Die Spezialisten der ZIT bringe ihre Erfahrungen regelmäßig bei Präventionsveranstaltungen ein. Oft ist es die Mischung aus Phänomenkenntnis und juristischem Fachwissen, die z.B. Eltern vorbeugend über die richtige Verhaltensweisen bei Abofallen oder Filesharing aufklären kann.

Bei der Strafverfolgung gemachte Beobachtungen über die typischen Verhaltensweisen von pädophilen Erwachsenen, die sich in sozialen Netzwerken als Kinder ausgeben, um so Kontakt zu ihren späteren kindlichen und jugendlichen Opfern zu erhalten, helfen dabei, in Öffentlichkeitsveranstaltungen brauchbare Hinweise zum Erkennen derartiger Täter zu geben und so die Medienkompetenz der Betroffenen zu stärken.

Neben der Vorbeugung durch die Vermittlung von Medienkompetenz gilt es aber auch, die Ermittler mit geeigneten Werkzeugen auszustatten, damit sie ihre Aufgabe erfüllen können. Um die vorhandenen Defizite der geltenden Gesetze zu beheben, hat Hessen in den letzten Jahren immer wieder gesetzgeberische Initiativen im Bereich von Cybercrimebekämpfung ergriffen, die sich mittelbar auch präventiv auswirken. Die Datenhehlerei wurde 2015 als Folge eines hessischen Vorstoßes in das StGB aufgenommen.

Weiterhin setze ich mich im Rahmen der Überarbeitung der Sexualstraftatbestände des Strafgesetzbuches vehement dafür ein, eine Versuchsstrafbarkeit für das Cybergrooming, also das gezielte Ansprechen von Kindern durch Erwachsene unter Nutzung digitaler Kommunikationsmittel zum Zwecke der Herbeiführung sexueller Handlungen, einzuführen. Die fehlende Versuchsstrafbarkeit führt dazu, dass unsere Bemühungen um eine effektive Bekämpfung dieses nur selten zur Anzeige gebrachten Deliktes mit Hilfe verdeckt agierender Polizeibeamter, die sich als Kinder ausgeben, häufig nicht von Erfolg gekrönt sind. Kommt es bei Internetkontakten des Pädokriminellen mit den verdeckten Ermittlern nicht zu expliziten sexuellen Handlungen des Täters oder fordert dieser nicht unmittelbar zur Vornahme derselben durch das vermeintliche Kind auf, ist dies als untauglicher Versuch noch nicht strafbar. Gerichte weigern sich in diesen Fällen regelmäßig, Durchsuchungsbeschlüsse zu erlassen. Hier muss weiter auf die Bundesregierung eingewirkt werden, um das Gesetz nachzubessern.

Aktuell hat Hessen daneben die effektive Bekämpfung der sogenannten „Botnetzkriminalität“ in den Fokus genommen. Als ein „Botnetz“ bezeichnet man eine große Anzahl von mit dem Internet ständig oder zeitweise verbundener Computer, die – von ihrem rechtmäßigen Nutzer unbemerkt – mit Schadprogrammen infiziert sind und daher einzeln oder in ihrer Gesamtheit einer fremden Kontrolle unterliegen.

Große Botnetze umfassen mehrere Millionen Opferrechner, die von dem jeweiligen sie kontrollierenden Täter einzeln oder zusammen ferngesteuert werden können. Botnetze sind auch Handelswaren, die über kriminelle Märkte im Internet in Gänze oder in Teilen

verkauft, verliehen oder vermietet werden. Sie stellen eine der wichtigsten Täterinfrastrukturen im Bereich der Cyberkriminalität dar. Botnetze werden genutzt zum Versenden von Spam-Emails, zur Begehung von Onlinebankingbetrug, zur Verschleierung des Standortes von Servern mit kriminellen Inhalten oder für Angriffe auf Webseiten, die diese unerreichbar machen, sogenannte „Distributed-Denial-of-Service-[DDoS]-Attacken".

Die derzeit verfügbaren Rechtsnormen §§ 303a, 303b StGB, die zur Bekämpfung der Botnetzkriminalität herangezogen werden können, sind im Kern fast 30 Jahre alt. Die Verurteilungszahlen nach diesen Normen sind gering, weil ihre Konzeption der Schutzgüter zu kompliziert und durch die heutige Realität überholt ist. Hessen wird daher noch vor der Sommerpause einen Gesetzentwurf für eine neue Strafnorm in den Bundesrat einbringen, die bereits das schlichte Gebrauchsrecht an IT-Systemen, unabhängig davon, ob bereits Daten auf diesen Systemen verändert, ausgespäht oder zerstört worden sind, einem strafrechtlichen Schutz unterstellt. Auch soll die heimliche Infiltration eines IT-Systems bereits ohne das Hinzutreten weiterer Voraussetzungen, also der schlichte digitale Hausfriedensbruch, bestraft werden.

Wie ich schon seit langem betone, muss das deutsche Strafrecht den Schritt ins 21. Jahrhundert vollziehen und auf die neuen Gegebenheiten und die damit einhergehenden neuen Kriminalitätsformen reagieren. So kann eine zeitgemäße Kriminalprävention wirksam flankiert und den Gefahren, die die digitale und vernetzte Welt für den Einzelnen und für Unternehmen birgt, wirkungsvoll begegnet werden.

Inhalt