Bund Deutscher Kriminalbeamter

Der BDK zu Besuch bei dem 2. Trierer Sicherheitstag

10.07.2015

Am 2. Juli 2015 fand der 2. Trierer Sicherheitstag statt. Schwerpunktthema in diesem Jahr war „Cybercrime“.

Bereits in der Begrüßungsrede machte Herr Polizeipräsident Lothar Schömann deutlich, dass das Thema Cybercrime in einer hochtechnisierten, allseits vernetzten Welt, von wachsender Bedeutung ist. Erst langsam wächst das Bewusstsein der Nutzer von IT-Endgeräten für IT-Probleme und die IT-Sicherheit.

Die Präsidentin der ADD, Frau Dagmar Barzen, sowie der Oberbürgermeister der Stadt Trier, Herr Wolfram Leibe, betonten in ihren Beiträgen, dass IT-Störfälle und Cybercrime keine Seltenheit mehr in heimischen Unternehmen, Behörden, Institutionen oder einfachen Haushalten sind, sondern eine alltägliche Realität. Weitere Referenten stellten dar, dass 8 von 10 heimischen Unternehmen in der Vergangenheit bereits einmal mit sog. „Störfällen“ ihrer IT zu tun hatten. Die häufigsten Probleme entstanden dabei durch Schadsoftware aus dem Internet (Viren, Trojaner) und aufgrund technischer Störungen wie Netzwerkausfällen. Die Zahl der Hacking-Attacken steigt bundesweit weiter an (derzeit 10% im Vergleich zum Vorjahr). Die Folgen von Ausfällen der IT können sehr weitreichend sein. Behörden sind nicht oder nur unzureichend arbeitsfähig (s. Ausfall Zulassungsstellen Mitte Juni); Unternehmen erleiden hohe finanzielle Einbußen, Image-Probleme, usw. Dr. Markus Mavany (Uni Trier) wies in seinem Vortrag zur strafrechtlichen Verfolgung von IuK-Kriminalität auf das enorme Dunkelfeld durch versuchte und erfolgreiche Angriffe hin. So wird nicht jede Phishing-Mail vom Empfänger gleich zur Anzeige gebracht, viele Romance-Skimming Fälle werden seitens der Opfer allein aus Scham verschwiegen und Unternehmen schweigen, um ihre Kundenbeziehungen nicht zu gefährden. Dr. Mavany stellt klar: Cybercrime ist ein weltweites Phänomen mit ganz pragmatische Probleme für die Strafverfolger: Wie ist die Zuständigkeit geregelt? Wo ist der Tatort? Auf irgendeiner Südseeinsel, von wo die letzte zurückverfolgbare IP stammt sicherlich nicht! Wie ist die Strafbarkeit im tangierten Drittland geregelt, um ein Rechtshilfeersuchen erfolgreich durchführen zu können? Wo liegt die Cloud, auf der gestohlene Daten gespeichert sind und wie muss der richterliche Beschluss aussehen, um die Daten zu beschlagnahmen? Wie ist die Kommunikation mit international agierenden Unternehmen rechtlich geregelt? Beispielsweise Facebook, Google, Apple, Amazon. Dies sind nur einige Fragen, die Ermittler sich stellen und beantworten müssen, um effektiv Strafverfolgung zu betreiben. Ebenso ist die rechtliche Einordnung der Tatbegehung in bestehende - zum Teil antiquierten - Straftatbestände nicht einfach. **Die größte Schwierigkeit, so Dr. Mavany, besteht darin, die Vorgehensweise der Täter zu verstehen, rechtlich einzuordnen und im Verfahren beweiskräftig vorzubringen. Hierzu bedarf es einer speziellen kriminalistischen und technischen Ausbildung. Auch Triers Oberbürgermeister Wolfram Leibe sieht die Politik aufgefordert, die Polizei so auszustatten, dass man dem Gegner auf Augenhöhe begegnen könne.**

Zum gleichen Ergebnis kamen Herr Jürgen Schüler, Projektleiter KOMZET von der HWK Rheinhessen, in seinem Vortrag über „IT-Sicherheit“ und Kriminalrat Jochen Bäcker, LKA Rheinland-Pfalz, in seinem Vortrag „Cyberunsicherheit und Phänomene“. Beide beleuchteten diverse Angriffsszenarien, Strategien und Methoden der Tatbegehung und skizzierten damit Täter, die über ein sehr hohes Fachwissen verfügen. IT-Sicherheitsprobleme müssen mehr aus technischer, rechtlicher und organisatorischer Sicht betrachtet werden. Dieses Ergebnis der Tagung zeigt sich auch im „Global Economic Crime Survey“ aus dem Jahr 2014, in dem Cybercrime nicht nur als ein technisches Problem angesehen wird, sondern als ein strategisches, menschliches und ein prozessuales Problem (PwCIL 2014).

Die Zusammenfassung zeigte eindrucksvoll die aktuelle Situation. Der BDK weist schon seit geraumer Zeit auf Ermittlungs- und Bearbeitungsmängel bei der Cybercrime hin und belegt damit, dass die Polizei in Rheinland-Pfalz nicht ausreichend genug auf die aktuellen und kommenden Problemstellungen aufgestellt ist.[1]

---

[1] Siehe BDK Info:

http://www.bdk.de/lv/rheinland-pfalz/aktuelles/cybercrime-2013-ist-die-polizei-richtig-aufgestellt