BLK: Cybersicherheit und Cybercrime

Datum: **Do, 22.09.2016 – 15:30 Uhr – 16:00 Uhr , HS 0.18**

Referent: **Rainer Franosch, Oberstaatsanwalt, Referatsleiter Cybercrime und IT-Sicherheit, Hessisches Ministerium der Justiz**

Protokoll: **Dominique Bosle**

Der Referent machte auf die Existenz eines themenbezogenen Referates aufmerksam.

Hinsichtlich der sog. 'Underground Economy' gab er zu verstehen, dass auf Täterseite regelmäßig weder das erforderliche technische Wissen und die Erfahrung, noch die notwendige technische und finanzielle Infrastruktur bestünde.

Gezeigt wurden verschiedene Screenshots von Websites aus dem sog. DARKNET, welches weder technisch noch juristisch definiert sei.
Veranschaulicht wurden außerdem anhand von Bildern Kategorien wie 'TOR – The Onien Router' mit Dreifachverschlüsselung und 'TOR Hidden Services: The Dark Net'.
Der Referent beleuchtete damit Strukturen und Erscheinungsformen organisierter Cyberkriminalität.

Als Problem stellten sich u.a. versteckte Server dar.

Insbesondere habe der Drogenhandel in jener Szene große Ausmaße angenommen. So sei anzunehmen, dass 1/3 des einstigen Straßenhandels im Freistaat Bayern nunmehr im Darknet stattfindet.
Daneben würden beispielsweise gefälschte Banknoten, Personalausweise und Waffen auf diesem Wege gehandelt.

Der Referent stellte dar, dass die Täter betreffende Ware an unbewohnte Adressen oder Paketstationen versendeten, um ungestört agieren zu können.

Die Taten beschränkten sich jedoch keineswegs auf den Handel mit den vorgenannten Gegenständen, sondern mündeten bereits in Szenarien, die ohne das Darknet in dieser Form nicht denkbar seien:

2014 habe es wohl den ersten deutschen Fall (Hessen) gegeben, wo eine Ausschreibung bezüglich der Suche eines Auftragskillers stattfand. (Stichwort 'QuickKill')
Dieser Fall wurde nur deswegen aufgeklärt, weil das Opfer überlebte und zur Klärung des Falles beitragen konnte.

Nicht als aussichtslos beschrieb der Referent die Ermittlungsarbeit, was insbesondere den Bereich der Kinderpornografie beträfe.

Anhand eines Bildes wurden die 'Crime Areas' aufgezeigt, nämlich 1. 'Crime as a service' und 2. 'Malware' (Stichwort 'Trojaner').

Hierbei wurde bekannt, dass beispielsweise für den Einsatz von Trojanern sogar eine Support-Hotline bestanden habe. Service mithin inklusive.

Als Zwischenfazit machte der Referent klar, dass sich jedes Unternehmen und die öffentliche Verwaltung überlegen müsse, wie es/sie sich gegen Angriffe absichern könne.

Hessen habe es u.a. innerhalb der Justiz Mitarbeitern untersagt, fahrlässig auf allenmöglichen Websites zu surfen.

Es ginge jedoch nicht nur um die Frage des Schutzes, sondern auch um die Frage der strafrechtlichen Verfolgung:

Der Referent stellte kurz einige Normen (u.a. § 202a StGB, § 303a StGB, § 303b StGB, Art. 2 des Budapester Übereinkommens) vor, um zu dem Schluss zu kommen, dass jene ungenügend bzw. untauglich seien um den Problemen Herr zu werden.

Als Reaktion sei am 17.06.2016 eine Gesetzesinitiative zum 'Digitalen Hausfriedensbruch' (als § 202b StGB) eingebracht worden, nachdem bereits 2015 die Datenhehlerei gesetzlich verankert wurde.