Bund Deutscher Kriminalbeamter

Fachtagung „Cyberbedrohung und Cyberschutz für Kommunen – informiert – wachsam – gewappnet“ am 20. April 2023 an der Hochschule der Polizei Rheinland-Pfalz

21.04.2023

BDK Rheinland-Pfalz informiert!

Auf Einladung von Herrn Innenminister Michael Ebling wurde die Fachtagung „Cyberbedrohung und Cyberschutz für Kommunen“ am 20. April an der Hochschule der Polizei Rheinland-Pfalz durchgeführt. Vor dem Hintergrund der deutlichen Zunahme von Bedrohungen gegenüber Kommunen und kommunalen Unternehmen durch Cyberangriffe in den vergangenen Jahren war es dem Innenminister ein persönliches Anliegen, über die aktuelle Sicherheitslage und die Möglichkeiten, Cyberangriffe abzuwehren, zu informieren.

Der BDK Rheinland-Pfalz hatte die Organisation und Durchführung der Veranstaltung bereits im Vorfeld begrüßt, da sich die Notwendigkeit nicht nur aus den Befunden und Empfehlungen der AG Kriminalitätsbekämpfung ergeben hat, sondern sich auch in dem seit geraumer Zeit bestehenden Positionspapier des BDK anlässlich des 50jährigen Bestehens widerspiegelt. Die Überlegungen zur Einrichtung einer Organisationseinheit zur Bekämpfung der Cybercrime in den Polizeipräsidien untermauern dies.

In der Fachtagung konnten Vertreter und Vertreterinnen aus dem Bundesamt für Verfassungsschutz, des Bundeskriminalamtes und des Landeskriminalamtes Rheinland-Pfalz ihre Expertisen unter Beweis stellen. Zudem berichtete Landrat Clemens Körner eindrucksvoll über den Cyberangriff auf die Verwaltung des Rhein-Pfalz-Kreises. Herr Christian Klaus der DigiFors GmbH referierte über Interventionsmöglichkeiten und -grenzen nach bzw. bei einem Cyberangriff.

Die Grundproblematik der Cyberspionage und Cybersabotage ist nicht wirklich neu und war von je her besorgniserregend. Ebenso ist seit längerem klar, dass Täter und Tätergruppierungen schnellere und professionellere Entwicklungszyklen zu verzeichnen haben als Strafverfolgungsbehörden, nicht zuletzt auch deshalb, weil sie schlussendlich über deutlich höhere finanzielle Möglichkeiten und Ressourcen verfügen können.

So führt Herr Sinan Selen des Bundesamtes für Verfassungsschutz aus, dass keine Entspannung zu erwarten ist. Die Gefahr der Destabilisierung durch Sabotagen steigt. Staatliche Akteure „choreografieren“ mit, was die Handlungsmöglichkeiten krimineller Strukturen unkalkulierbar erweitert. Die aktuellen weltpolitischen Entwicklungen, insbesondere aus dem Russland-Ukraine-Konflikt, belegen dies.

Herr LKD Martin Nolte vom Bundeskriminalamt greift dies in seinem Vortrag ebenfalls auf. Die Professionalität der Täter in der Underground Economy nimmt zu, auch durch die Verfügbarkeit von technischen Mitteln, die auch der Laie mit qualitativ hochwertigen Ergebnissen nutzen kann, ohne selbst auf eine hochqualifizierte Kompetenz zurückgreifen zu müssen. In vielerlei Hinsicht sind zudem die Cybercrime-Dienstleistung „buchbar“ („Crime as a Service“) oder es ist auf entsprechenden kriminellen Foren ein Informations- und Erfahrungsaustausch möglich. Über Franchise-Modelle entwickelt sich hier eine kriminelle Dienstleistungsindustrie. Erlangte Daten werden zudem mehrfach verwertet und somit die Verwertungskette durch entsprechende Verteilungswege verlängert. Für den Einsatz von unterschiedlichen Schadprogrammen werden Anti-Viren-Testsysteme angeboten mit Hilfestellungen für die Täter, ihre inkriminierten Programme resistent und damit leistungsfähiger zu machen. Das BKA empfiehlt schließlich den Geschädigten, u. a. entsprechende Notfallpläne zu erstellen und die Prozesse für die Datenübernahme an die Polizei technisch wie rechtlich vorzubereiten. Hierzu gehört, neben der schnellen Einrichtung von Krisenstäben, die Festlegung und Gewährleistung von schnellen Erreichbarkeiten auch zur Polizei sowie von festen Ansprechpartnern für die Polizei. Ein Kontakt zwischen Tätern und geschädigten Kommunen bzw. Unternehmen soll nicht erfolgen.

Zwar wurde mit der Zentralen Ansprechstelle Cybercrime (ZAC) eine entsprechende fachliche Organisationseinheit bereits geschaffen, diese reicht aber aus Sicht des BDK Rheinland-Pfalz mit ihrer bisherigen Ausprägung nicht aus, zumal es entsprechender korrespondierender Einheiten bei den Polizeipräsidien bedarf. Nur so kann eine schnelle qualifizierte Intervention und Betreuung betroffener Kommunen und kommunaler Unternehmen gewährleistet werden. Dies wird insbesondere dann erforderlich sein, wenn eine 24/7-Intervention, auch an Wochenenden, beabsichtigt ist, da sich die Täter erfahrungsgemäß bei ihren Spionage- und Sabotageaktionen eben zielgerichtet nicht an Regelarbeitszeiten der Polizei orientieren.

Der Wunsch nach einem schnelleren Reaktionsmuster der Polizei ist nachvollziehbar, da die Schäden für die betroffenen Verwaltungen und Unternehmen im Vergleich zu einer Lösegeldzahlung von Minute zu Minute steigen und letztendlich kostenintensiv bleiben.

Die Teilnehmerinnen und Teilnehmer der Fachtagung profitierten von den kurzweilig vorgetragenen Erfahrungen und Empfehlungen aus der Sicht eines unmittelbar Betroffenen. Der Hinweis auf die Notwendigkeit einer 24/7-IT-Bereitschaft in der Verwaltung und damit verbundenen Schwierigkeiten des Tarifrechts sowie der Bewertung der in Rede stehenden Stellen nach EG 10 TV-L traf den Nerv vieler Tagungsteilnehmerinnen und -teilnehmer. Die Polizei Rheinland-Pfalz kennt dieses Problem

nur zu gut! Die Probleme bei der Besetzung entsprechender Stellen im Bereich IT aufgrund mangelnder Bewerbungen, wie aktuell bei den Ausschreibungen zu den „Datenanalysten“, lassen sich nicht wegdiskutieren.

Hier müssen u. a. entsprechende Anreize geschaffen, das Tarifrecht überarbeitet und haushalterische Voraussetzungen geschaffen werden, um Fachpersonal rekrutieren und vorhandenes Fachpersonal langfristig binden zu können.

Der BDK Rheinland-Pfalz fordert hier ein zeitnahes Handeln und unterstützt die entsprechenden Empfehlungen der AG Kriminalitätsbekämpfung hierzu ausdrücklich!

Autor: KD Ingolf Hubert