Bund Deutscher Kriminalbeamter

Kritische Betrachtung der Bekämpfung der Cybercrime aus Sicht eines fachkompetenten Kriminalbeamten

30.04.2016

Der Autor bezieht sich auf einen Beitrag im NDR-Nordmagazin vom 27.04.2016, ab 19:30 Uhr, der sich mit den gerade in Stralsund stattfindenden „Danziger Gesprächen“ und deren Thema „Mobile Daten. Mobile Bürger. Mobile Polizei.“ befasste.

Dazu die Sichtweise aus dem Blickwinkel eines Ermittlers für Cybercrime:

Die Problematik Cybercrime wurde durch das Ministerium für Inneres und Sport bereits 2014 erkannt und es wurde eine Projektgruppe unter Federführung des Landeskriminalamtes Mecklenburg-Vorpommern mit Beteiligung aller Dienststellen im Rahmen einer Umfrage installiert. Auch eine Bund-Länder-Umfrage floss in das Ergebnis der „Vorschläge für eine Cybercrime-Bekämpfungsstrategie der Landespolizei Mecklenburg-Vorpommern“ vom 05.11.2014 ein.

Ein aus meiner Sicht durchdachtes Konzept mit einem „Nachteil“: Es verlangt nach Geld und Personal.

Dessen Bereitstellung und Umsetzung versagt bislang die Landespolitik, und um nicht ganz so schlecht dazustehen, wird die Masse der Cybercrime-Delikte in der PKS einfach nicht erfasst, da die Tatorte mehrheitlich nicht in Deutschland liegen.

Das durch dieses Deliktfeld Schäden im 2stelligen Milliardenbereich entstehen, wird einfach nicht publiziert. Man stelle sich vor, in Deutschland würden jährlich für 20 Milliarden Euro Fahrzeuge entwendet?! (Quelle)

Dafür hören wir von unserem Innenminister Caffier:“...die Polizei ist gut aufgestellt“. Die Tatsachen sprechen ein anderes Bild. Der Express „Cybercrime“ ist vor Jahren abgefahren und wir versuchen diesen mit einem Bummelzug einzuholen.

Hier eine unvollständige Aufzählung:

Unzureichend geschulte Beamte erfassen Anzeigen falsch und unvollständig. Dadurch entsteht ein nicht aufzuholender Verzug in der Bearbeitung, insbesondere wegen der fehlenden Vorratsdatenspeicherung. IP-Adressen werden je nach Provider bis zu 7 Tage beauskunftet.

Die Ermittler haben nicht den nötigen Wissensstand, zumal die Angriffe auf Netze und Clients immer perfider werden – die Angriffsszenarien wechseln ständig. Das nötige Wissen um diese Dinge muss ich mir als Ermittler autark aneignen, dafür fehlt mir aber die Zeit. Die Notwendigkeit einer kontinuierlichen Aus- und Fortbildung wurde zwar erkannt, aber in der Realität nicht umgesetzt. Die Fachhochschule Güstrow ist dazu nicht in der Lage und für externe Lehrgänge werden entsprechende Kosten nicht eingeplant.

Ein Tipp für Enthusiasten: Das Hasso-Plattner-Institut bietet hier kostenfreie Onlinekurse an.

Dass andere Länder eine andere Sicht auf diese Dinge haben beweist Thüringen. Hier werden für 4 Polizeivollzugsbeamte die Studienkosten für das berufsbegleitende Studium an der Hochschule Mittweida zum B.Sc. für IT-Forensik/ Cybercreme übernommen.

Auf technischer Seite fehlt es an Hard- und Software sowie an einem anonymisierten Internetzugang. So haben Ermittler keine administrativen Rechte auf den Auswertesystemen, um mit open-Source-Tools zu arbeiten, es fehlt an Linux-basierten Systemen und kompromittierte Rechner können nicht untersucht werden, weil der Internet-Anschluss über das Dienststellennetz erfolgen müsste. Von kompromittierten Smartphone ganz zu schweigen. Hier müsste die Untersuchung im Dezernat 55 unseres Landeskriminalamtes erfolgen, aber welcher Geschädigte verzichtet über Monate oder Jahre auf sein Telefon? Im Grunde genommen hebeln so Verwaltungsvorschriften den § 163 StPO aus.

Mit Wirkung zum 04.01.2016 wurde die Verwaltungsvorschrift - II 440c - II-203-30430-2011/029-033 – in Kraft gesetzt. Damit wurde ein Teil der „Konzeption Cybercrime“, also die zentrale Bearbeitung der Delikte umgesetzt, aber auch das Kind mit dem Bad ausgeschüttet. Die Kriminalpolizeiinspektion Rostock als Fachdienststelle ist mit der zeitnahen und damit erfolgversprechenden Abarbeitung der Massendelikte überfordert. Bekanntlich leidet Qualität unter Quantität. Hier hätte auch eine personelle Zuweisung erfolgen müssen. Daran werden auch die in dem o.g. Beitrag genannten Seiteneinsteiger nach § 16 PolLaufbVO M-V nichts ändern, deren polizeiliche Ausbildung erst noch erfolgen muss. Auf der anderen Seite hat man durch eine offensichtlich falsche Personalentscheidung eine Koryphäe an „Verizon Enterprise Solutions Deutschland“ verloren.

Aus meiner Sicht kann nur die zügige und vollständige Umsetzung der „Vorschläge für eine Cybercrime-Bekämpfungsstrategie der Landespolizei Mecklenburg-Vorpommern“ zur Verbesserung dieser Situation führen. Letztendlich muss sich das in einem neuen Fachkommissariat für Cybercrime wiederspiegeln. Diese Umsetzung würde auch die Prognosen für die nahe Zukunft reflektieren. Die Risiken werden zunehmen durch:

- Bargeldlose und NFC-Zahlungsverfahren,
- Smartphones, Smart Watches, Health- und Fitness-Tracker, Smart Home,
- Smart Meter und Onlinesynchronisierung,
- Cloud-Computing,

- Internet of Things.

Schon jetzt ist es möglich, Fahrzeuge und Flugzeuge zu hacken.

Wenn wir uns heute ein Landeskriminalamt mit allen Dienstleistungen als ein Gebäude mit der Größe X vorstellen, werden in etwa fünf Jahren drei Gebäude von gleicher Größen daneben stehen. Diese werden bezeichnet sein mit „facebook“, „Ransomware“ und „Kryptologie“. So die Aussagen der Prof. Labudde und Hummert von der Hochschule Mittweida.

Jeder weitere Tag ohne ausreichend kompetentes Personal und die erforderlichen technischen Voraussetzungen entfernt uns weiter vom gesetzlichen Auftrag, auch die unter dem Begriff „Cybercrime“ zusammengefassten Straftaten in erforderlicher Weise aufzudecken und zu verfolgen.

Geredet wurde wahrlich genug, handeln wir endlich.

NDR Mediathek