Bund Deutscher Kriminalbeamter

Grundsätzliche Überlegungen zur Cyberkriminalität aus Anlass der Datenveröffentlichungen von Politikern u. a.

09.01.2019

Seit Tagen herrscht große Aufregung und Betroffenheit über die von einem 20jährigen per Twitter verbreiteten privaten Daten von Politikern, Journalisten und Prominenten.

Die größte Erregung zeigen dabei ausgerechnet die Politiker, deren politisches Programm davon geprägt ist, eine effektivere Bekämpfung u. a. der Cyberkriminalität möglichst zu verhindern. Sie erweckten bislang regelmäßig den Eindruck, die Rufe der Kriminalisten nach effektiveren Ermittlungsinstrumenten oder effizienteren Softwaresystemen seien in Wahrheit Ausdruck eines ohnehin vorhandenen, orwellschen Totalüberwachungstriebes. Die eigene Betroffenheit lässt sie das augenscheinlich derzeit für einen Moment vergessen.

Der politische Fahrplan verlief erwartungsgemäß: zunächst Fehlersuche bei den staatlichen Sicherheitsbehörden gepaart mit hilflos anmutenden Forderungen nach höherer Datensicherheit. Nach Ergreifung des Täters binnen 48 Stunden, werden die Ermittlungsbehörden nun pflichtgemäß gelobt. Ich kann mich leider nicht davor bewahren, dass sich mir angesichts der ein oder anderen öffentlichen Äußerung wechselseitig der Magen umdreht und mir die Zornesröte ins Gesicht steigt. Ganz aktuell liegt das vor allem daran, dass die aktuellen Opfer der Straftaten nur deswegen eine so hohe Aufmerksamkeit genießen, weil es sich um Politiker, Journalisten und andere Prominente handelt. Wir reden über inzwischen alltäglich gewordene Kriminalität. Jeden Tag werden deutsche Bürgerinnen und Bürger Opfer von Cyberkriminalität. Zahllose Taten hinterlassen schwere psychische oder materielle Schäden. Darunter sind Kinder als Missbrauchsopfer, deren Bild- und Videoaufnahmen rund um den Globus gehandelt und getauscht werden und die auf diese Weise über die eigentliche Tat hinaus immer wieder aufs neue viktimisiert werden. Darunter sind ältere Menschen, die erpresst werden, weil von den Tätern glaubhaft behauptet wird, sie in kompromittierender Lage mit der eigenen Webcam gefilmt zu haben. Ebenfalls darunter sind abertausende namenlose Bürgerinnen und Bürger, deren Identitäten gestohlen wurden. Leider verfügten all diese Opfer bislang nicht die über eine ansatzweise vergleichbare Lobby, wie die jetzigen. Was sagt das eigentlich über den Zustand unserer Gesellschaft aus und wer müsste sich eigentlich dafür momentan gewaltig schämen?

Ich möchte aber die Gelegenheit ergreifen und einige ausgesuchte, wichtige Grundsatzfragen der Bekämpfung der Cyberkriminalität beleuchten.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI)

Die Zeit ist überfällig, einmal die gesetzlich zugewiesene Rolle des BSI, seine Einbindung in die Sicherheitsarchitektur sowie sein tatsächliches Agieren genauer unter die Lupe zu nehmen. Dabei ist für mich die in die Kritik geratene Presse- und Öffentlichkeitsarbeit seines Präsidenten von untergeordneter Bedeutung. Wichtiger erscheint mir die Informationspolitik gegenüber den übrigen Sicherheitsbehörden. Diese wird bislang nur hinter den Kulissen bemängelt. Sie ist jedoch von viel erheblicherer Relevanz für die nationale Sicherheit.

Schon seit längerer Zeit erhalte ich von Kolleginnen und Kollegen der Kriminalpolizei nicht nur positive Rückmeldungen, wenn ich mich mit ihnen über ihre Zusammenarbeit mit dem BSI unterhalte. Nicht selten besteht offenbar deutlicher Anlass zur Kritik. In seinem Leitbild *„Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft“* und bei öffentlichen Stellungnahmen trägt das Amt ein nicht zu übersehendes, teilweise übersteigertes Selbstbewusstsein vor sich her. In der Praxis jedoch klaffen die hierdurch erzeugten Erwartungen und die Wirklichkeit auseinander. Das Verhältnis des BSI zu den Strafverfolgungsbehörden ist leider kein störungsfreies. Es gibt keine gesetzliche normierte Pflicht des BSI, die Strafverfolger über ihm bekannt gewordene Cyberstraftaten zu informieren. Folglich geschieht dies in vielen Fällen auch nicht in wünschenswertem Maße.

Die Politik sollte sich entscheiden, welche Art Cybersicherheitsbehörde sie möchte und wie diese in die Sicherheitsarchitektur eingefügt werden soll. Für mich jedenfalls steht fest, dass mindestens für schwerwiegende Cyberkriminalität eine gesetzlich normierte Pflicht festgeschrieben werden muss, die Strafverfolgungsbehörden hierüber zu informieren. Da sich die Behörde leider auch bei der Herausgabe von Beweismitteln an die Strafverfolger systematisch sperrt, sollte auch dieser wichtige Punkt der Zusammenarbeit künftig im Gesetz klar geregelt sein.

Die Sicherheitsarchitektur

Die deutsche Sicherheitsarchitektur ist in wesentlichen Teilen antiquiert, in anderen Bereichen schlicht unfertig. Die europäische Sicherheitsarchitektur wird kaum öffentlich diskutiert. Einige Thesen und Forderungen:

I. Das Bundeskriminalamt fordert derzeit eine gesetzliche Zuständigkeit zur Gefahrenabwehr in Bezug auf die Cyberkriminalität. Das wirft viele Fragen auf, da der zweite Schritt vor dem ersten gefordert wird. So einfach, wie in der realen Welt, lassen sich präventive Eingriffsmaßnahmen nicht umsetzen. Schritt eins sollte daher eine gemeinsam mit den Ländern entwickelte nationale Cyber-Präventionsstrategie sein.

II. Es ergibt keinen Sinn, dass bei größeren Cyberstraftaten, die mehrere Bundesländer betreffen, mehrere Landeskriminalämter am selben Fall arbeiten. Die bereits jetzt schon vorhandenen, herausragenden Fähigkeiten einzelner Landeskriminalämter in bestimmten Ermittlungsfeldern, sollten diese auch anderen Ländern zur Verfügung stellen. Die konzeptionellen Rahmenbedingungen sollten zwischen Bund und Ländern verbindlich festgeschrieben werden.

III. Für besonders schwerwiegende Cyberkriminalität ist eine Kompetenz der künftigen Europäischen Staatsanwaltschaft anzustreben. Europol sollte stärker als derzeit in die operativen Ermittlungen der Europäischen Staatsanwaltschaft einbezogen

werden dürfen - in Kooperation mit den Mitgliedsstaaten. Europol ist auf diesem Weg, u. a. bei der Bekämpfung der Cyberkriminalität sowie des Internationalen Terrorismus und der Organisierten Kriminalität, zu einem **European Bureau of Investigations (EUBI)** weiterzuentwickeln.

IV. Eines der Hauptprobleme bei Cyberattacken besteht darin, dass zu Beginn eines größeren Angriffs, sehr häufig nicht festgestellt werden kann, wer der Angreifer ist. Steckt ein anderer Staat mit seinem Geheimdienst oder von ihm beauftragte Gruppierungen dahinter, sind es Kriminelle oder gar Terroristen? In bestimmten Fällen kann es unklar sein, ob es sich um einen Fall der inneren oder der äußeren Sicherheit handelt. Das seit 2011 beim BSI eingerichtete Cyber-Abwehrzentrum ermöglicht ausschließlich einen Austausch der Bundesbehörden. Die im föderalen Deutschland hauptzuständigen Länderbehörden stehen vor der Tür. Die Bekämpfung der Cyberkriminalität ist zunächst einmal nicht originäre Bundeskompetenz.

V. Für die Fragen des Datenschutzes sowie der Datensicherheit enthält die Datenschutzgrundverordnung klare Regeln, die u. a. die Anbieter sozialer Netzwerke in die Pflicht nehmen. Wenn immer wieder Nutzern von Internetdiensten oder sozialen Plattformen vorgeworfen wird, sie seien bei Passwortvergaben zu nachlässig, so fällt dieser Vorwurf unmittelbar auf die Anbieter zurück. Sie sind zur Herstellung eines angemessenen Sicherheitsniveaus verpflichtet. Sollten sie dieser Verpflichtung nicht nachkommen, sieht die Datenschutzgrundverordnung einschneidende Sanktionen vor, die bis zu 2 %, in schwerwiegenden Fällen bis zu 4 %, des globalen Jahresumsatzes erreichen können. Dieses recht neue Recht sollte auch zur Anwendung gebracht werden.

VI. Ich kann es nicht aussparen: Wir verfügen über massiv zu wenig Personal, das zur Bekämpfung der Cyberkriminalität eingesetzt werden kann und können die an uns gestellten Erwartungen daher nur zu einem Bruchteil erfüllen. Alle Länder müssen Anstrengungen in einer neuen Dimension entfalten, um unsere Reihen schnellstmöglich zu verdichten. Insbesondere bei den Ermittlungskräften benötigen wir hochspezialisierte Kriminalbeamtinnen und -beamte. Jedes Bundesland sollte daher Möglichkeiten eines Quereinstiegs für vorqualifizierte Bewerber eröffnen.

Sebastian Fiedler