Cyber-Security als Rechtsstaatspflicht

Matthias Klatt 2019-11-26T14:00:41

Joint Symposium on the Internet Governance Forum of the United Nations 2019

Von MATTHIAS K. KLATT

Einer der Schwerpunkte des „Internet Governance Forums“ der Vereinten Nationen 2019 ist das Thema „Security & Safety“ – Fragen der Datensicherheit und der Sicherheit von Infrastrukturen im digitalen Zeitalter. Dieses Thema ist für Individualpersonen von besonderer Bedeutung, doch auch staatliche Institutionen und Organe sollten dieses Thema auf der Agenda haben. Denn ein aktueller Fall aus Berlin zeigt, dass die Sicherheit staatlicher informationstechnischer Systeme elementare Verfassungsprinzipien unmittelbar berühren kann. Die Errichtung und Sicherung der IT-Systeme ist eine grundlegende Vorbedingung für einen funktionsfähigen Rechtsstaat und sollte daher von Regierungen, (Justiz-)Verwaltung und Gesetzgeber stärker in den Blick genommen werden.

Kammergericht Berlin offline

Am 25. September 2019 wurde das KG Berlin vom IT-Dienstleistungszentrum Berlin informiert, dass mittels eines Trojaner-Angriffs über eine fingierte E-Mail die Schadsoftware „Emotet“ in das IT-System des Gerichts gelangt war. Das Kammergericht wurde daraufhin vom Internet und wenige Tage später auch zusätzlich vom Landesnetz getrennt. Damit wurde vor allem ein Übergriff des Trojaners auf IT-Systeme der Berliner Verwaltung verhindert. Laut Mitteilung des KG Berlin kam es zwar nicht zu einem Datenverlust, jedoch ist durch die Trennung vom Netzwerk für die Richter und Verwaltungsmitarbeiter ein Zugriff auf die Daten nur von sog. „Auskunfts-PCs“ aus möglich. Ende Oktober begann die Verwaltung damit, neue E-Mail-Adressen einzurichten.

Laut KG Berlin war das Gericht zum Zeitpunkt des Hacker-Angriffs mit einer professionellen Antivirensoftware ausgestattet, die dem letzten technischen Stand

entsprach. Versäumnisse sind dabei aber offensichtlich: So gehört das KG erst „künftig“ zum IT-Dienstleistungszentrum Berlin und führt – früher als bisher geplant – jetzt eine VPN-Technik ein, um ein sicheres Arbeiten der Mitarbeiter zuhause erreichen zu können. Warum diese Maßnahmen nicht bereits früher vorgenommen wurden, ist nicht verständlich.

Die (potentiellen) Auswirkungen der Schadsoftware „Emotet“ sind dabei gewaltig: So kann das Adressbuch des infizierten Rechners gelesen werden, um anderen Personen unbemerkt infizierte E-Mails zu senden. Eine volle Kontrolle über die gespeicherten Daten ist möglich. Nun besteht die Gefahr erst einmal nicht für Akten aus Prozessen und laufenden Verfahren – der deutschen Papierwut sei Dank, ist die eAkte noch weit entfernt. Doch ist nicht auszuschließen, dass auf den Servern, etwa in E-Mails, wichtige Informationen über Verfahren und Beteiligte abgreifbar sind. Und: Sollten Richter Dokumente auf der lokalen Festplatte ihres Dienstrechners gespeichert haben ist darauf kein Zugriff möglich, diese Daten könnten sogar dauerhaft verloren sein.

Der Arbeitsalltag der Richter leidet unterdessen stark: Ein Zugriff auf Datenbanken von Urteilen und Literatur ist nicht mehr möglich, vielfach bleibt nur der Gang in die Bibliothek und diese sind bei Gerichten oft nicht ausreichend ausgestattet. Der Justizsenator spricht von „schwierigen Bedingungen“; es gebe „nichts schönzureden“. Dieser Zustand soll bis in das Jahr 2020 andauern. Dass all dies Verfahrensverzögerungen verursachen wird, steht außer Frage.

Effektiver Rechtsschutz erfordert IT-Sicherheit

Bei einer Betroffenheit der justiziellen IT-Sicherheit sind automatisch elementare Verfassungsgüter berührt. Dies zeigt: Cyber-Security ist kein Thema für Technik-Nerds, sondern wichtige Vorbedingung eines effektiven Rechtschutzes in einem modernen Rechtsstaat im digitalen Zeitalter.

Das Rechtsstaatsprinzip aus Art. 20 GG Abs. 2 und 3 GG verlangt einen wirkungsvollen Rechtsschutz und damit eine umfassende tatsächliche und rechtliche Prüfung des Streitgegenstandes, sowie eine verbindliche gerichtliche Entscheidung (hier, S. 291). Der Verfahrensbeteiligte kann dieses Verfassungsprinzip mittels Art. 2 Abs. 1 GG auch beim BVerfG geltend machen. Hinsichtlich der Verwaltungsgerichtsbarkeit ergeben sich die rechtsstaatlichen Grundsätze aus Art. 19 Abs. 4 GG. Darüber hinaus unterbindet das Recht auf den gesetzlichen Richter aus Art. 101 Abs. 1 S. 2 GG eine formelle Justizverweigerung mangels Bedeutung der Sache oder Zeit (*Schulze-Fielitz*, in: Dreier GG-Kommentar, Bd. III, Art. 101 Rn. 58). Eine Ausprägung des Rechtsstaatsprinzips ist das Gebot des fairen Verfahrens (hier, S. 257f.): International in Art. 6 Abs. 1 EMRK und Art. 47 S. 1 GRCh verankert, verlangt es nach der Rechtsprechung des BVerfG eine „angemessene Beschleunigung des Verfahrens“ (hier). Neben Versäumnissen der Prozessparteien, seien dabei zunächst die Verzögerungen zu beachten, die durch die Justiz selbst verursacht worden seien. In einer verfassungsgerichtlichen Kammer-Entscheidung findet sich dieser Hinweis sehr deutlich (Rn. 10):

> „*Dagegen kann sich der Staat nicht auf solche Umstände berufen, die in seinem Verantwortungsbereich liegen. Er muss alle notwendigen Maßnahmen treffen, damit Gerichtsverfahren zügig beendet werden können*."

Diese Auslegung verbietet dem KG Berlin eine Berufung darauf, dass der Angriff auf das IT-System ein externer Faktor sei und zu Verzögerungen geführt habe. Denn: nimmt man den effektiven Rechtsschutz ernst, müssen die Justiz und deren Verwaltung auch *präventive* Schutzmaßnahmen ergreifen, um eine angemessene Arbeitsweise der Richter zu ermöglichen. Dazu gehört im digitalisierten Zeitalter auch eine angemessene IT-Sicherheit. Besonders pikant: Nur einen Tag vor der Attacke auf das KG hatte das Bundesamt für Sicherheit in der Informationstechnik vor einer Welle von Angriffen gewarnt. Dessen Leitung zeigte sich ungeduldig: „*Man kann es nur gebetsmühlenartig wiederholen: Viele dieser Schäden sind vermeidbar, wenn IT-Sicherheitsmaßnahmen konsequent umgesetzt werden!*"

Angemessene Ausstattung der Gerichte

Wichtiger Teil des grundgesetzlichen Rechtsstaatsprinzips ist der Grundsatz des *effektiven* Rechtsschutzes, der unzumutbare Erschwerung des Zugangs zu Gerichten verbietet. Daraus lässt sich auch ableiten, dass die Organisation und Arbeitsweise von Gerichten für diesen rechtsstaatlichen Auftrag angemessen sein muss. Effektive Gerichtsbarkeit ist dabei nicht nur eine Frage der *zeitlich* angemessenen Bewältigung der Verfahren, sondern insbesondere eine der *Ausstattung* der Gerichte. Neben einer angemessenen Personalversorgung, die nicht mit Experimenten wie etwa dem "Richter auf Zeit" kompensiert werden sollte (dazu *Klatt*, NVwZ 2019, 374 ff.), ist es auch angezeigt, das Richteramt so auszugestalten, dass die rechtsstaatlichen Aufgaben im digitalen Zeitalter gut und effektiv erfüllt werden können. Dazu muss es in einem ersten Schritt gehören, eine angemessene digitale Infrastruktur aufzubauen. Kommunikation mit Prozessbeteiligten, Recherche für Urteilsentwürfe, Information über aktuelle Rechtsentwicklungen, Dokumentenerstellung – all dies sind Elemente richterlicher Tätigkeiten, die sich mittlerweile mittels digitaler Infrastruktur vollziehen können (und sollten). Hard- und Software müssen dafür auf einem angemessenen Stand sein, der derzeit nicht erreicht ist. Darüber hinaus müssen auch Richter und Verwaltungsmitarbeiter sensibilisiert und umfassend geschult werden. Beim KG Berlin mehrten sich Berichte, dass es die Richter mit der Sicherheit von Daten nicht allzu genau nähmen.

Handlungsbedarf für Regierung und Verwaltung

Gefragt sind Regierungen, Verwaltung und Gesetzgeber, die nicht lediglich gefährliche Brandherde löschen, sondern präventiv Feuerschutztüren und Feuerlöscher bereitstellen müssen. Das ist nicht nur rechtspolitisch wünschenswert, sondern verfassungsrechtlich geboten. Bis 2026 sollen alle Rechtsverfahren und die Kommunikation zwischen den Berliner Gerichten und Verfahrensbeteiligten rein elektronisch ablaufen, bis 2022 die eAkte eingeführt werden. Damit steigen natürlich auch die Anforderungen an die IT-Sicherheit und die Ausstattung der Gerichte, die

derzeit noch nicht erreicht ist. Ganz zu schweigen davon, dass die Praxis von der derzeitigen wissenschaftlichen Diskussion – von praktischen Überlegungen wie in anderen Staaten ganz zu schweigen – über das Potential von Künstlicher Intelligenz in der Justiz (instruktiv *Dreyer/Schmees*, CR 2019, S. 758 ff.) noch meilenweit entfernt ist.

Zitiervorschlag: Klatt, Matthias K., Cyber-Security als Rechtsstaatspflicht, JuWissBlog Nr. 101/2019 v. 26.11.2019, https://www.juwiss.de/101-2019/.