IT-SICHERHEIT IN DER JUSTIZ – WEGE AUS EINER DROHENDEN KRISE

Stefan Hessel / Andreas Rebmann

Associate, reuschlaw Legal Consultants, 66117 Saarbrücken, DE
stefan.hessel@reuschlaw.de; https://www.reuschlaw.de

Wissenschaftlicher Mitarbeiter, Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes, 66123 Saarbrücken, DE
andreas.rebmann@uni-saarland.de; https://legalinf.de/rebmann

Schlagworte: ***IT-Sicherheit, Datenschutz, Justiz, Digitalisierung, Justizgewährungsanspruch***

Abstract: *Der Beitrag analysiert welche Bedrohungen für die IT-Sicherheit durch die Digitalisierung der Justiz entstehen. Er unterscheidet dabei zwischen zufälligen und zielgerichteten Angriffen. Darüber hinaus arbeitet der Beitrag heraus, dass die Justiz nicht nur die DSGVO, sondern auch aufgrund des Justizgewährungsanspruchs zur Gewährleistung von IT-Sicherheit verpflichtet ist. Sodann untersucht der Beitrag anhand eines Einzelfallbeispiels, wie gut die deutsche Justiz vor Angriffen geschützt ist, bevor abschließend Lösungsansätze für die Verbesserung der IT-Sicherheit in der Justiz unterbreitet werden.*

1. Einleitung

Mit der Einführung von elektronischem Rechtsverkehr und e-Akte wird die Digitalisierung der bundesdeutschen Justiz massiv ausgebaut. In Zukunft soll dadurch eine Justiz entstehen, die sich moderne Zugangsmöglichkeiten und Verfahrensabläufe zu Nutze macht und dadurch einen bürgerfreundlichen Zugang ermöglicht.[1] Doch die Digitalisierung der Justiz verknüpft die Arbeitsfähigkeit der Gerichte auch mit der Funktionsfähigkeit ihrer Computersysteme. Deutlich wird dies beispielsweise an einem Angriff mit der Schadsoftware Emotet, der im Herbst 2019 das Kammergericht Berlin wochenlang in seiner Arbeitsfähigkeit einschränkte.[2] Ein zentraler Bestandteil für den Erfolg der Digitalisierung in der Justiz ist daher die Gewährleistung von IT-Sicherheit. Deren Umsetzung läuft aber – wie der Fall des Kammergerichts ebenfalls zeigt – alles andere als optimal.[3] Ausgehend davon erläutert der Beitrag, welchen Herausforderungen sich die Justiz im digitalen Raum gegenüber sieht, wer für die Bewältigung dieser Herausforderungen verantwortlich ist und welche Wege die Justiz aus dem Minenfeld der Bedrohungen führen können.

2. Die Justiz in der digitalen Welt

Prinzipiell sind die IT-Systeme aller für die Rechtsprechung verantwortlichen Behörden, also der Justiz, den selben Gefahren und Angriffsszenarien ausgesetzt, wie jedes andere IT-System auch. Hinzu kommen spezifisch auf die Justiz und ihre Infrastruktur abzielende Angriffe. Diese resultieren aus der besonderen Stellung der Justiz und der damit einhergehenden Bedeutung für eine Vielzahl von Personen. Diese Bedeutung schlägt

[1] So etwa die niedersächsische Justizministerin Barbara Havliza zum «Masterplan Digitalisierung» der niedersächsischen Landesregierung, https://www.mj.niedersachsen.de/startseite/themen/digitalisierung/masterplan-digitalisierung-in-der-justiz-151498.html – zuletzt abgerufen am 31.10.2019.

[2] Kiesel, Berliner Kammergericht hantierte leichtfertig mit sensiblen Daten, Tagesspiegel.de, 16.10.2019, https://www.tagesspiegel.de/berlin/nach-trojaner-angriff-berliner-kammergericht-hantierte-leichtfertig-mit-sensiblen-daten/25119536.html – zuletzt abgerufen am 31.10.2019.

[3] Ebenda.

sich auch in der analogen Welt nieder und so ist es traurige Realität, dass Mitarbeiter der Justizbehörden immer wieder Ziel von teils körperlichen Angriffen, in jüngerer Zeit vor allem durch sog. Reichsbürger, werden.[4]

2.1. Die Justiz als Beifang von Malware-Kampagnen

Durch die zunehmende Digitalisierung entstehen jedoch neue Angriffsszenarien in bisher nicht erreichbaren Größenordnungen. Viele Angriffswellen auf IT-Systeme erfolgen nicht auf ein bestimmtes Ziel, sondern in Folge von Massenangriffen. Hierbei haben die Angreifer in den meisten Fällen finanzielle Interessen.[5] Auch wenn diese Art der Angriffe nicht auf die Justiz als solches abzielt und ihre IT-Systeme nur Beifang eines größeren Angriffs sind, können solche Szenarien erhebliche Probleme für die Behörden bedeuten. Befallene IT-Systeme können die Arbeit der gesamten Behörde zum Erliegen bringen. Dass solche Angriffe häufiger werden, ist bei einer zunehmenden Digitalisierung nur folgerichtig. Durch steigende elektronische Kommunikation erhöht sich auch die Zahl der Einfallstore für digitale Angriffe. Allein durch die Einführung des besonderen elektronischen Anwaltspostfachs (beA) wird ein Teil der bisher analog durchgeführten Kommunikation auf die digitale Ebene verlagert.[6] Darüber hinaus gilt für digitale Angriffe auf die Justiz ein wesentlicher Grundsatz der IT-Sicherheit: Eine Veränderung des Kosten-Nutzen-Risikos schafft eine neue Ausgangslage für Angreifer. Durch die zunehmende Digitalisierung der Justiz wird die potentielle Beute bei einem erfolgreichen Angriff deutlich größer. So macht die Digitalisierung der Justiz bisher analoge Daten für einen Angreifer zumindest potentiell auf digitalem Wege verfügbar. Hinzukommt, dass Dokumente in zunehmendem Maße nicht mehr auf dem jeweiligen Rechner der bearbeitenden Person gespeichert werden, sondern an zentraler Stelle. Daher ist es bei einem erfolgreichen Eindringen in ein IT-System deutlich einfacher, eine Vielzahl an Dokumenten zu kopieren.[7] Müsste ein Angreifer beim Einbruch in ein Gerichtsgebäude stapelweise Akten heraustragen, können im digitalen Bereich Akten schnell in großer Zahl vervielfältigt werden.

2.2. Gezielte Angriffe auf die Justiz

Die zunehmende Digitalisierung der Justiz führt jedoch auch zu einer Steigerung von gezielten Angriffen.[8] Auch hier gilt das für Angreifer günstigere Kosten-Nutzen-Verhältnis bei digitalen Angriffen. Die Gründe für gezielte Angriffe auf Justizsysteme können hierbei vielfältig sein: Spaß an der Zerstörung, Rache aufgrund von subjektiv erlittenem Unrecht oder Vorteilsgewinnung durch unberechtigten Zugriff auf nicht-öffentliche Informationen sind nur einige Beispiele.[9] Zielgerichtete Angriffe auf staatliche Infrastrukturen und Behörden sind nichts neues. Terroristische Anschläge auf Justizgebäude oder Personen sind insbesondere noch aus Zeiten der RAF bekannt. Doch auch in jüngerer Zeit verüben Angreifer Attacken auf staatliche Infrastruktur, regelmäßig auch auf digitalem Wege. So wurde etwa im Dezember 2015 die ukrainische Energieversorgung Ziel eines digitalen Angriffs, in dessen Folge über mehrere Stunden ein weitreichender Blackout eintrat.[10] Terrorgruppen wie der Islamische Staat haben in der Vergangenheit ebenfalls ihre Angriffskapazitäten im Bereich des digitalen Terrorismus unter Beweis gestellt. Dies belegt exemplarisch ein Angriff auf den französischen Fernsehsender TV5Monde, in dessen Verlauf über mehrere Stunden das gesamte TV-Programm des Senders abgeschaltet wurde und Rechner-Systeme lahmgelegt wurden. Ähnliche Attacken sind auch bei

4 Schuldt, Zuschauer legen Verhandlung gegen «Reichsbürgerin» lahm, Nordkurier.de, 27.03.2019, https://www.nordkurier.de/mueritz/richter-fordert-polizeischutz-an-2731622703.html – zuletzt abgerufen am 31.10.2019.

5 Rossow/Sorge, Schadsoftware: Ein Problem (auch) für Juristen?, jM 2018, S. 7 (S. 8).

6 Rossow/Sorge, Schadsoftware: Ein Problem (auch) für Juristen?, jM 2018, S. 7 (S. 9).

7 Vogelgesang, Datensicherheit und IT-Sicherheit in der Justiz, jM 2018, S. 2 (S. 4).

8 Ebenda, S. 6f; Rossow/Sorge, Schadsoftware: Ein Problem (auch) für Juristen?, jM 2018, S. 7.

9 Rossow/Sorge, Schadsoftware: Ein Problem (auch) für Juristen?, jM 2018, S. 7 (S. 8).

10 Krempl, Stromausfall in der Ukraine augenscheinlich durch Hacker ausgelöst, heise.de, 06.01.2016, https://www.heise.de/security/meldung/Stromausfall-in-der-Ukraine-augenscheinlich-durch-Hacker-ausgeloest-3063343.html – zuletzt abgerufen am 31.10.2019.

der Justiz denkbar. So lässt sich auch im bereits erwähnten Fall des Kammergerichts Berlin auf mögliche Konsequenzen verweisen, wenn IS-Anhänger aus gehackten Akten an die persönlichen Daten von Zeugen in Terrorverfahren kämen: «Das bekommt eine besondere Relevanz, weil das Kammergericht in Berlin die erste Instanz für sämtliche Fälle von Terrorismus ist, beispielsweise für Rückkehrer aus dem «Islamischen Staat» (IS).»[11] Auch Gefahren ganz anderer Art für die Justiz können durch die zunehmende Digitalisierung entstehen. So hat sich 2014 in England ein Häftling selbst aus dem Gefängnis entlassen, indem er mit einer Fake-E-Mail-Adresse und gefälschten Mails die Gefängnisleitung instruierte.[12] Aktuelle Beispiele des sog. CEO-Frauds zeigen, wie weit sich solche Täuschungssysteme bereits entwickelt haben. Beim CEO-Fraud wird von den Tätern eine Anweisung durch den Unternehmenschef – meist per e-Mail – imitiert. Ein ähnlicher Fall wäre problemlos mit einer KI-generierten Stimme des Haftrichters vorstellbar, bei der eine Software durch Machine Learning Verfahren eine Stimme imitiert. Somit kann die Glaubwürdigkeit einer gefälschten E-Mail noch unterstützt werden. Doch auch mit simpleren Methoden können Justizstellen angegriffen werden. Sog. Reichsbürger nutzten bereits öffentlich zugängliche Informationen, um diese für «Fahndungsaufrufe» nach Richtern in sozialen Medien zu verwenden.[13] Dies zeigt die Omnipräsenz der Digitalisierung unserer Gesellschaft. Wenn sich die Justiz konzeptuell mit diesem Thema befasst, ist dies nicht als Insellösung möglich, sondern muss eine ganzheitliche Betrachtungsweise beinhalten.[14]

3. IT-Sicherheit als justizielle Verantwortung

In Anbetracht der dargestellten Bedrohungslage stellt sich die Frage, inwieweit und auf welcher Grundlage die Justiz zur Umsetzung von IT-Sicherheit verpflichtet ist. Trennen lässt sich insoweit zwischen dem Schutz von personenbezogenen Daten und der Gewährleistung der Funktionsfähigkeit der Gerichte im Allgemeinen.

3.1. IT-Sicherheit durch das Datenschutzrecht

Der Schutz personenbezogener Daten erfolgt einfach gesetzlich in der Regel durch das Datenschutzrecht. Insoweit ist zunächst von Interesse, welchen datenschutzrechtlichen Regelungen die Justiz unterworfen ist. Darüber hinaus kommt aber auch der Frage, welche Stelle innerhalb der Justiz als Verantwortlicher im Sinne des Datenschutzrechts für die Einhaltung der Regelungen verantwortlich ist, eine wesentliche Bedeutung zu.

3.1.1. Anwendbarkeit der DSGVO auf die Justiz

Der europäische Gesetzgeber hat die Verpflichtung der Justiz zum Schutz von personenbezogenen Daten in Erwägungsgrund (EG) 20 der Datenschutzgrundverordnung (DSGVO) ausdrücklich vorgesehen. Die Justiz muss sich daher, unabhängig von einigen Sonderregelungen, bei der Verarbeitung von personenbezogenen Daten inhaltlich vollumfänglich an der DSGVO messen lassen.[15] Soweit die Justiz personenbezogene Daten verarbeitet, hat sie diese daher nach Art. 32 DSGVO mit angemessenen Maßnahmen nach dem Stand der Technik zu schützen, wobei jedoch keine konkreten Maßnahmen vorgeschrieben sind. Besonders hohe Schutzanforderungen gelten für die Verarbeitung von besonders sensiblen personenbezogenen Daten, wie

[11] Benrath, Wie ein Trojaner das höchste Gericht Berlins lahmlegte, Frankfurter Allgemeine, 20.10.2019, https://www.faz.net/aktuell/wirtschaft/diginomics/emotet-wie-ein-trojaner-das-hoechste-gericht-berlins-lahmlegte-16442702.html – zuletzt abgerufen am 31.10.2019.

[12] Welt.de, Häftling entlässt sich selbst mit gefälschter E-Mail, welt.de, 31.03.2015, https://www.welt.de/vermischtes/kurioses/article138951065/Haeftling-entlaesst-sich-selbst-mit-gefaelschter-E-Mail.html – zuletzt abgerufen am 31.10.2019.

[13] Vogel/Wangemann, Reichsbürgerin bedroht Brandenburger Richter, Märkische Allgemeine, 19.01.2019, https://www.maz-online.de/Lokales/Ostprignitz-Ruppin/Neuruppin/Reichsbuergerin-bedroht-Richter-und-Staatsanwaelte – zuletzt abgerufen am 31.10.2019.

[14] BSI-Standard 200-2, Version 1.0, S. 11.

[15] Engeler, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, C.H.BECK, München 2019, § 22 Datenschutz in der Justiz, Rn. 6.

zum Beispiel Gesundheitsdaten, im Sinne von Art. 9 Abs. 1 DSGVO.[16] Die Justiz darf diese Daten zwar auf Grundlage des Art. 9 Abs. 2 lit. f DSGVO verarbeiten,[17] muss dabei jedoch den erhöhten Schutzanforderungen Rechnung tragen. Hinsichtlich der Gewährleistung von IT-Sicherheit gelten für die Justiz vor dem dargestellten Hintergrund keine Erleichterungen oder gesetzlichen Ausnahmen zur Absenkungen des Schutzniveaus. Ein zentraler Unterschied bei der Umsetzung und Einhaltung des geltenden Datenschutzrechts ergibt sich jedoch aus Art. 55 Abs. 3 DSGVO. Dieser beschränkt die Zuständigkeit der nationalen Aufsichtsbehörden soweit eine Datenverarbeitung durch ein Gericht im Rahmen einer justiziellen Tätigkeit vorgenommen wird.[18] Für diese Kategorie von Verarbeitungsvorgängen sollen nach EG 20 DSGVO besondere Stellen im Justizsystem geschaffen werden. Nach dem Willen des Gesetzgebers ist die Aufgabe dieser gerichtsinternen Datenschutzaufsicht insbesondere, die Einhaltung des Datenschutzrechts sicherzustellen. In der Sache regelt Art. 55 Abs. 3 DSGVO daher nur, welche Kontrollinstanz die Einhaltung der DSGVO in der Justiz überwacht. Er ändert jedoch nichts daran, dass die DSGVO auf den Kernbereich der richterlichen Arbeit anwendbar ist.[19] Für die Strafgerichte gilt auch unter Berücksichtigung der JI-Richtlinie[20] nichts anderes.[21]

3.1.2. Bestimmung der verantwortlichen Stelle

Die grundsätzliche Anwendbarkeit eines Gesetzes auf einen Sachverhalt führt jedoch nicht automatisch zur Einhaltung des Gesetzes. Aus diesem Grund ist die Frage, wer als Verantwortlicher für die Datenverarbeitung durch die Justiz anzusehen und damit nach Art. 24 Abs. 1 DSGVO zur Umsetzung der technischen und organisatorischen Maßnahmen zur IT-Sicherheit ist, keineswegs zu vernachlässigen. Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Soweit die Justizbehörden hierarchisch organisiert sind, ergeben sich zunächst keine Abweichungen im Vergleich mit Privatunternehmen.[22] Der Behördenleiter ist als Leiter einer nicht-öffentlichen Stelle im Sinne von § 2 Bundesdatenschutzgesetz (BDSG) gleich einem Geschäftsführer für die Datenverarbeitung innerhalb der Behörde verantwortlich.[23] Aus dem Grundsatz der richterlichen Unabhängigkeit gemäß Art. 97 Abs. 1 GG könnte sich jedoch für die Gerichte – nicht jedoch für die Staatsanwaltschaften, da diese in Deutschland grundsätzlich nicht unabhängig sind[24] – etwas anderes ergeben. Ausgehend davon wird teilweise vertreten, dass der einzelne Richter für die von ihm im Rahmen seiner Rechtsprechungstätigkeit vorgenommene Datenverarbeitung als Verantwortlicher anzusehen sei.[25] Dem wird jedoch zu Recht entgegenhalten, dass der Richter zwar die Datenverarbeitung praktisch vornehmen mag, jedoch insoweit trotz richterlicher Unabhängigkeit Teil des Gerichts als Organisationseinheit ist.[26] Im Ergebnis lässt sich daher festhalten, dass die Verantwortung für die Gewährleistung von IT-Sicherheit stets bei den Behördenleitern der jeweiligen Justizeinrichtungen liegt. Weitere Konstellationen wie eine gemeinsame Verantwortlichkeit mehrerer Akteure oder eine justizielle Auftragsverarbeitung sind in diesem Zusammenhang ebenfalls denkbar und möglich.[27]

---

16 Vogelgesang, Datensicherheit und IT-Sicherheit in der Justiz, jM 2018, S. 2 (S. 3).
17 Engeler, in: Specht/Mantz (Fn. 16), Rn. 7.
18 Ebenda, Rn. 8.
19 Ebenda.
20 Richtlinie 2016/680/EU, ABl. L 119/89.
21 Engeler, in: Specht/Mantz (Fn. 16), Rn. 10.
22 Schild, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 29. Edition, Stand 01.08.2019, C.H.BECK, München 2019, Art. 4 DSGVO, Rn. 88 f.
23 Ebenda.
24 Inhofer, in: Graf (Hrsg.), BeckOK GVG, 4. Edition, Stand 10.08.2019, C.H.BECK, München 2019, § 146 GVG Rn. 6 f.
25 Schild, in: Wolff/Brink (Fn. 23), Datenschutz bei Gerichten und Staatsanwaltschaften, Rn. 10.
26 Engeler, in: Specht/Mantz (Fn. 16), Rn. 27.
27 Engeler, in: Specht/Mantz (Fn. 16), Rn. 29 ff.

3.2. Verfassungsrechtliche Verpflichtung zur IT-Sicherheit

Die Verpflichtung der Justiz zur Gewährleistung von IT-Sicherheit durch die DSGVO ist in erster Linie durch den Anwendungsbereich der Verordnung selbst begrenzt. Sie gilt – wie bereits gezeigt – ausschließlich für die Verarbeitung von personenbezogen Daten. Eine generelle Verpflichtung, die Justiz vor digitalen Angriffen zu schützen, ergibt sich jedoch aus dem Justizgewährungsanspruch des Grundgesetzes. Dieser wird für den Rechtsschutz in öffentlich-rechtlichen Streitigkeiten durch Art. 19 Abs. 4 GG gewährleistet.[28] Für Streitigkeiten anderer Art, insbesondere zivilrechtliche, wird die Verpflichtung des Staates zur Bereitstellung einer Rechtsschutzmöglichkeit aus dem Rechtsstaatsprinzip in Verbindung mit Art. 2 Abs. 1 GG abgeleitet.[29] Der Justizgewährungsanspruch beinhaltet neben einem Grundrecht auf Individualrechtsschutz auch eine institutionelle Garantie.[30] Der Staat ist insoweit zur Schaffung einer Gerichtsbarkeit verpflichtet, die den grundgesetzlichen Rechtsschutzauftrag erfüllen kann.[31] Dies umfasst neben den organisatorischen und verfahrensmäßigen Voraussetzungen eines wirksamen Rechtsschutzes auch die finanzielle Basis.[32] Daraus lässt sich schlussfolgern, dass der Staat ein Mindestmaß an IT-Sicherheit in der Justiz zu gewährleisten hat, um die Funktionsfähigkeit der Gerichtsbarkeit sicherzustellen. Bei der Auswahl geeigneter Maßnahmen und deren konkreter Umsetzung ist der Gesetzgeber jedoch weitgehend frei.[33] Diese Gestaltungsfreiheit darf jedoch nicht darüber hinweg täuschen, dass ein klarer grundgesetzlicher Auftrag zum Schutz der Justiz vor digitalen Angriffen besteht.

4. Vorboten einer Krise

Aus einer Gegenüberstellung der klaren gesetzlichen Verpflichtung zur Gewährleistung von IT-Sicherheit in der Justiz einerseits und der dargestellten Bedrohungslage ergibt sich jedoch keineswegs ein zufriedenstellendes Bild. So sind zwar einerseits in den vergangenen Jahren vergleichsweise wenige Fälle von digitalen Angriffen auf die Justiz publik geworden, andererseits gibt es dazu jedoch auch kaum belastbare Zahlen.[34] Eine Analyse über den Stand der IT-Sicherheit in der Justiz soll daher an dieser Stelle anhand des bereits erwähnten Angriffs auf das Kammergericht Berlin im Herbst 2019 erfolgen.

4.1. Emotet – König der Schadsoftwaren

Der Angriff auf das Kammergericht wurde mit Hilfe von Emotet durchgeführt.[35] Dabei handelt es sich um eine Schadsoftware, die sich insbesondere durch das Verschicken von authentisch aussehenden Spam-Mails auszeichnet.[36] Um dieses Ziel zu erreichen, liest Emotet im Rahmen des sogenannten «Outlook-Harvesting» bestehende Kontaktbeziehungen und E-Mailinhalte aus den gehackten E-Mailpostfächern aus und verwendet diese als Vorlage für E-Mails an weitere potentielle Opfer.[37] Doch Emotet beschränkt sich nicht nur auf

---

[28] Huster/Rux, in: Epping/Hillgruber (Hrsg.), BeckOK Grundgesetz, 41. Edition, Stand 15.2.2019, C.H.BECK, München 2019, Art. 20 GG, Rn. 199.

[29] Ebenda.

[30] Schmidt-Assmann, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, 87. EL, März 2019, C.H.BECK, München 2019, Art. 19 Abs. 4 GG, Rn. 14.

[31] Ebenda.

[32] Ebenda.

[33] Enders, in: Epping/Hillgruber (Fn. 29), Art. 19 GG, Rn. 74 ff.

[34] Zahlen zu versuchten und erfolgreichen Angriffen auf die Justiz in Deutschland finden sich beispielsweise weder in den Jahresberichten des BSI zur IT-Sicherheit, noch in den Cybercrime-Lagebildern des BKA. Auch die EDV-Länderberichte der Bund-Länder-Kommission für Informationstechnik in der Justiz enthalten keine belastbaren Zahlen.

[35] Keilani, Berliner Kammergericht nicht vor 2020 wieder am Netz, Tagesspiegel.de, 24.10.2019, https://www.tagesspiegel.de/berlin/trojaner-angriff-berliner-kammergericht-nicht-vor-2020-wieder-am-netz/25146868.html – zuletzt abgerufen am 31.10.2019.

[36] BSI, Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html – zuletzt abgerufen am 31.10.2019.

[37] Ebenda.

das Auslesen von E-Mailkonten zum Zweck der weiteren Verbreitung.[38] Die Schadsoftware kann über das Nachladen von verschiedenen Modulen auch Ransomware-Angriffe durchführen oder mit der Schadsoftware Trickbot Zugangsdaten für Online-Banking ausspähen.[39] Darüber hinaus kann Emotet sich über Schwachstellen im sogenannten Server Message Block (SMB) Protokoll auch im lokalen Netzwerk ausbreiten.[40] Diese zahlreichen Schädigungsmöglichkeiten in Verbindung mit der automatisierten Generierung von authentischen SPAM-Mails macht Emotet so erfolgreich, dass er auch als König der Schadsoftwaren gilt.[41] Gleichwohl sind Betreiber von IT-Systemen der Schadsoftware keineswegs hilflos ausgeliefert. Die Erfolgsaussichten eines Emotet-Angriffs lassen sich vielmehr durch verschiedene Maßnahmen signifikant reduzieren.[42]

4.2. Veraltete Software

Eine dieser vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in diesem Zusammenhang als zwingend vorgesehene Maßnahme ist der Einsatz aktueller Software.[43] Das Kammergericht Berlin setzte bis zuletzt mit dem System AuLAK (Automation des Landgerichts, der Amtsgerichte und des Kammergerichts) jedoch eine Software ein,[44] die für den Einsatz mit Microsoft Word95 konzipiert wurde.[45] Dass das Problem veralteter Software im Justizkontext ein häufiges Problem ist, zeigt auch das beA. So bemängelte das von der Bundesrechtsanwaltskammer nach der vorläufigen Abschaltung des beA in Auftrag gegebene Sicherheitsgutachten ebenfalls den Einsatz von veralteten Softwareelementen.[46] Dies verweist auf ein zentrales Problem: Die Softwarelösungen sind oft abhängig von externen Software-Komponenten, die stetig weiterentwickelt werden. Notwendig ist also eine ständige Anpassung und Weiterentwicklung der Justiz-Software, die ihrerseits mit Kosten und Aufwand verbunden ist. Dies stellt die Justiz vor enorme Herausforderungen und so wundert es wenig, dass auch der Nachfolger von AuLAK, das System ForumSTAR, bereits auf veraltete Komponenten angewiesen sein soll.[47]

4.3. Backupstrategie und IT-Wildwuchs

Eine weitere Herausforderung für die Justiz, die sich am Fall des Kammergericht Berlin offenbart, ist eine ausreichende Backupstrategie. So wird es beim Kammergericht Berlin bis ins Jahr 2020 dauern, bis das Gericht wieder in einen normalen IT-Betrieb übergehen kann.[48] Bis dahin haben die Richter ausschließlich über sogenannte Notfall-PCs Zugriff auf ihre Daten.[49] Während der Zeitraum zur Wiederherstellung der Daten schon jetzt zu lange erscheint, muss jedenfalls bei Einführung der eAkte eine deutlich schnellere Wieder-

38 Ebenda.
39 Ebenda.
40 Ebenda.
41 Tremmel, «Emotet ist der König der Schadsoftware», golem.de, 17.10.2019, https://www.golem.de/news/bsi-praesident-emotet-ist-der-koenig-der-schadsoftware-1910-144480.html – zuletzt abgerufen am 31.10.2019.
42 BSI, Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html – zuletzt abgerufen am 31.10.2019.
43 Ebenda.
44 Kiesel/Keilani, IT-Katastrophe am Berliner Kammergericht kam mit Ansage, Tagesspiegel.de, 29.10.2019, https://www.tagesspiegel.de/berlin/experten-warnten-schon-2017-it-katastrophe-am-berliner-kammergericht-kam-mit-ansage/25163810.html – zuletzt abgerufen am 31.10.2019.
45 Bund-Länder-Kommission für Informationstechnik in der Justiz, EDV-Länderbericht Berlin, Stand: August 2019, https://justiz.de/BLK/laenderberichte/berlin.pdf – zuletzt abgerufen am 31.10.2019.
46 Secunet Security Networks AG, Technische Analyse und Konzeptprüfung des beA, Version 1.0, Stand. 18.06.2019, https://www.rak-sachsen.de/documents/2018/06/secunet-ag-gutachten-bea.pdf – zuletzt abgerufen am 31.10.2019.
47 Kiesel/Keilani, IT-Katastrophe am Berliner Kammergericht kam mit Ansage, Tagesspiegel.de, 29.10.2019, https://www.tagesspiegel.de/berlin/experten-warnten-schon-2017-it-katastrophe-am-berliner-kammergericht-kam-mit-ansage/25163810.html – zuletzt abgerufen am 31.10.2019.
48 Krempl, Emotet: Berliner Kammergericht bleibt bis 2020 weitgehend offline, heise.de, 25.10.2019, https://www.heise.de/newsticker/meldung/Emotet-Berliner-Kammergericht-bleibt-bis-2020-weitgehend-offline-4569544.html – zuletzt abgerufen am 31.10.2019.
49 Ebenda.

herstellung der Daten möglich sein. Das Sichern von Daten im Rahmen von Backups ist insoweit nur ein Teil der zu bewältigenden Aufgabe, da auch eine zeitlich angemessene Wiederherstellung möglich sein muss.[50] In einem gewissen Zusammenhang damit steht auch das Problem, dass Justizdaten oftmals auf Privatgeräten verarbeitet und dorthin mittels USB-Sticks transportiert werden.[51] Diese Implementierung des Konzepts von Bring-Your-Own-Device ist eine inakzeptable Gefahr für die IT-Sicherheit und daher – trotz der richterlichen Unabhängigkeit – zu Recht abzulehnen.[52] Bei genauerer Betrachtung des Vorfalls im Kammergericht Berlin lässt sich daher festhalten, dass die IT-Sicherheit der Justiz bisher nicht in ausreichendem Maße gewährleistet wird. Während grundsätzlich technische Lösungen für die Probleme vorhanden sind, fehlt es vielfach an Konzepten und noch häufiger an deren Umsetzung.

5. Lösungswege

Mit der Weiterentwicklung und Professionalisierung der Angriffe werden auch stetig Schutzmaßnahmen fortentwickelt. Der Kampf zwischen Angreifern und IT-Sicherheitsexperten gleicht einem ständigen Katz-und-Maus-Spiel. Gleichwohl existiert mittlerweile eine Vielzahl von technischen Lösungen, die geeignet sind, ein angemessenes IT-Sicherheitsniveau zu gewährleisten.[53] Rossow und Sorge verweisen jedoch völlig zu recht darauf, dass die technische Komponente nur ein Teil eines IT-Sicherheitskonzepts sein kann und der sog. Faktor Mensch eine ebenbürtige Rolle spielt. Gerade weil die technischen Sicherungsmaßnahmen immer besser werden, nehmen Angreifer vermehrt die menschliche Komponente als schwächstes Glied der IT-Sicherheitskette an. Hierbei wollen sich Angreifer die technische Unbedarftheit vieler Nutzer zum Vorteil machen und Schritte, die von einem Überwachungssystem als verdächtig eingestuft werden würden, vom Anwender ausführen lassen.

5.1. Grundverständnis schaffen

Die hier erkannten Probleme können jedoch nicht nur der Unbedarftheit vieler Anwender zugeschrieben werden. Neben der Eigenverantwortung der Nutzer besteht – wie bereits beschrieben – auch eine Verantwortung der Behörden, für die IT-Sicherheit zu sorgen. Dazu gehört auch, Mitarbeiter in die Lage zu versetzen, ein System sicher zu verwenden. Wie diese Aufgaben umgesetzt werden sollen, wird meist jedoch gar nicht festgehalten. Insbesondere bei der menschlichen Komponente der IT-Sicherheit herrscht oftmals Unverständnis über elementare Konzepte der IT-Sicherheit.[54] Damit sind weniger fehlende Fertigkeiten in Bezug auf technische Lösungen gemeint, sondern viel mehr eine fehlende Einsicht in die Bedeutung des Themas. Schlecht oder nicht geschulte Behördenleiter, Richter, Staatsanwälte und sonstige Justizbedienstete können auch eine ablehnende Haltung gegenüber IT-Sicherheitsmaßnahmen einnehmen. Insofern ist es bemerkenswert, dass Mitarbeiterschulungen zur IT-Sicherheit in der Justiz bisher nicht flächendeckend etabliert scheinen. Fehlt die Einsicht von Verantwortlichen und Mitarbeitern, verliert auch ein gutes IT-Sicherheitskonzept seine Wirkung, da die geplanten Maßnahmen nicht umgesetzt werden.[55]

---

50 BSI, Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html – zuletzt abgerufen am 31.10.2019.

51 Keilani, Berliner Kammergericht nicht vor 2020 wieder am Netz, Tagesspiegel.de, 24.10.2019, https://www.tagesspiegel.de/berlin/trojaner-angriff-berliner-kammergericht-nicht-vor-2020-wieder-am-netz/25146868.html – zuletzt abgerufen am 31.10.2019.

52 Krüger/Möllers/Vogelgesang, Richterliche Unabhängigkeit und Bring Your Own Device (BYOD) – Weg in die Zukunft oder unvertretbares Sicherheitsrisiko?. In: Schweighofer, Kummer, Hötzendorfer, Sorge (Hrsg.), Trends und Communities der Rechtsinformatik. Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017, books@ocg.at, Wien 2017, S. 295 (S. 302).

53 Siehe auch Rossow/Sorge, Schadsoftware: Ein Problem (auch) für Juristen?, jM 2018, S. 7 (S. 9f.).

54 Trend Micro, Interne Kommunikation stellt größte Herausforderung für Cybersicherheit dar, trendmicro.com, 29.01.2019, https://www.trendmicro.com/de_de/about/newsroom/press-releases/2019/20190129-interne-kommunikation-stellt-groesste-herausforderung-fuer-cybersicherheit-dar.html – zuletzt abgerufen am 31.10.2019.

55 BSI Standard 200-2, Version 1.0, S. 162.

5.2. IT-Sicherheit als Prozess

Zu den elementaren Prinzipien eines erfolgreichen IT-Sicherheitskonzepts zählt u.a. das Thema IT-Sicherheit als fortlaufenden Prozess zu verstehen. IT-Sicherheit ist kein statischer Zustand, der, einmal erreicht, dauerhaft fortbesteht, sondern ein Prozess, der ständigen Anpassungen unterworfen ist. So wie sich Angriffsszenarien ständig ändern und Angreifer ihre Methoden weiterentwickeln, so werden auch Verteidigungsstrategien laufend angepasst und Änderungen in der Strategie müssen umgesetzt werden. Deutlich wird dies beispielsweise an veralteten Vorstellungen über die Sicherheit von Passwörtern, bei denen sich die Empfehlungen mittlerweile quasi um 180 Grad gewendet haben.[56] Wurde noch vor einigen Jahren ein regelmäßiger Wechsel aller Passwörter und eine möglichst zufällige Kombination aus Zeichen empfohlen, wird heute ein Wechsel nur noch im Falle einer Kompromittierung bzw. nach Neueinrichtung als notwendig erachtet. Auch langen Passwörtern, die aus mehreren Wörtern bestehen, wird u.a. wegen der besseren Merkbarkeit der Vorzug gegenüber zufälligen Zeichenketten gegeben. Das BSI verweist für das IT-Sicherheitsmanagement auf den sogenannten PDCA-Zyklus.[57] Der PDCA-Zyklus beschreibt den Sicherheitsprozess dabei als vierstufigen Lebenszyklus mit den Stufen Plan (P, Planung), Do (D, Umsetzung), Check (C, Erfolgskontrolle) und Act (A, Verbesserung). Besonderen Wert wird hierbei auf die Punkte Erfolgskontrolle (C) und daraus resultierenden Verbesserungen (A) gelegt. Ohne regelmäßige Überprüfung kann die Wirksamkeit der technischen und organisatorischen Maßnahmen zum Schutz der IT-Systeme auf Dauer nicht sinnvoll sichergestellt werden.[58]

5.3. Kommunikation von IT-Sicherheit

Das bereits oben angesprochene Grundproblem mangelnder Einsicht in das Thema IT-Sicherheit kann auch mit mangelhafter Kommunikation zusammenhängen: In der Justiz werden Mitarbeiter oftmals noch viel zu wenig in die Thematik IT-Sicherheit eingebunden. Abgesehen von den IT-Abteilungen wird das Thema in der Realität eher als für die eigene Arbeit irrelevant wahrgenommen. Für ein funktionierendes IT-Sicherheitskonzept ist es jedoch essentiell, dass alle Mitarbeiter, ob im IT-Bereich tätig oder nicht, mit den Grundlagen der IT-Sicherheit vertraut sind.[59] Jede Kette ist nur so stark wie ihr schwächstes Glied und mit der Omnipräsenz von vernetzten Computerarbeitsplätzen kann jeder Mitarbeiter durch eine unbedachte Aktion einen IT-Sicherheitsvorfall auslösen. Breit angelegte Schulungen sensibilisieren die Mitarbeiter und befähigen sie, IT-Sicherheit umsetzen zu können.[60] Aber auch unabhängig von Schulungen muss deutlich werden, dass das Thema IT-Sicherheit auf jeder Ebene und für jeden Mitarbeiter relevant ist. Die Einrichtung von IT-Abteilungen, Informationssicherheitsbeauftragten und Datenschutzbeauftragten bedeutet nicht, dass das Thema IT-Sicherheit dorthin abgeschoben werden kann. Die besten IT-Sicherheitsexperten sind machtlos, wenn der betroffene Mitarbeiter die Grundlagen der IT-Sicherheit nicht versteht und sich darüber hinwegsetzt. Doch auch für die Kommunikation im Schadensfall gilt, dass alle Mitarbeiter sensibilisiert werden müssen. Gesetzliche Meldepflichten können nicht eingehalten werden, wenn den Verantwortlichen nicht bewusst ist, wann eine solche Meldepflicht eintritt und wem gegenüber eine Meldung zu erfolgen hat.

56 NIST Special Publication 800-63B, Digital Identity Guidelines, June 2017.

57 BSI, IT-Grundschutz-Schulung, Der Sicherheitsprozess, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_2_Sicherheitsmanagement/Lektion_2_01/Lektion_2_01_node.html – zuletzt abgerufen am 31.10.2019.

58 Ebenda.

59 BSI Standard 200-2, Version 1.0, S. 34.

60 Ebenda.

6. Fazit und Ausblick

Insgesamt muss festgehalten werden, dass bekannte Probleme bei der IT-Sicherheit in der Justiz immer wiederzukehren scheinen, obwohl technische und organisatorische Maßnahmen existieren und eine gesetzliche Pflicht zur Umsetzung dieser besteht. Vor diesem Hintergrund muss der bundesdeutschen Justiz ein eher schlechtes Zeugnis ausgestellt werden. Weitere erfolgreiche Angriffe sind zu befürchten. Um dies zu vermeiden sind nicht nur IT-Sicherheitskonzepte sondern auch deren Umsetzung notwendig. Inwieweit die Eigenverantwortung der Gerichte insbesondere auch im Hinblick auf die datenschutzrechtliche Selbstkontrolle auf den Prüfstand gehört oder ein IT-Sicherheitsgesetz für die Justiz erforderlich ist, muss die Zukunft zeigen.