Prof. Dr. Alexander Roßnagel
Daniel Wilke, LL.M.

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
im Forschungszentrum für Informationstechnikgestaltung (ITeG)
der Universität Kassel

Projekt VoIPS – Rechtssicheres Archivieren von Internettelefonie

Rechtsgemäße Gestaltung der EMA E-Mail Archive Appliance

Kassel, den 3. April 2009

Inhalt:

Die Archivierung aufgezeichneter über das Internet geführter Telefongespräche im Projekt VoIPS basiert auf der Technik der EMA E-Mail Archive Appliance (im Folgenden: EMA). Diese ist ein aus Hardware und Software bestehendes System zur Archivierung von E-Mails und wird im Folgenden auch als Archivierungsserver bezeichnet. Die Gesprächsinhalte sollen in gleicher Weise gespeichert und verwaltet werden wie die mit der EMA-Technologie archivierten E-Mails. Die aufbewahrten Telefoniedaten werden daher im Hinblick auf Datenschutz und Datensicherheit den gleichen Risiken unterliegen wie die archivierten E-Mails. Die im Projekt VoIPS entwickelte Lösung zur Archivierung der Telefoniedaten kann daher nur rechtsgemäß sein, wenn auch die E-Mail-Archivierung mittels der EMA-Technologie den rechtlichen Anforderungen an solche Systeme entspricht. Im Folgenden ist daher zu untersuchen, ob die EMA-Technik den Anforderungen des Daten- und Geheimnisschutzes und einer sicheren Aufbewahrung genügt. Weiterhin ist zu prüfen, welchen Beweiswert die mittels EMA archivierten E-Mails haben.

1 Funktionsweise der EMA im Überblick

Die archivierende Stelle verwendet einen Archivierungsserver, mit dem eine Vielzahl von Arbeitsplatzrechnern über das Internet verbunden ist. Die im Folgenden als Nutzer bezeichneten Mitarbeiter der archivierenden Stelle versenden und empfangen an den Arbeitsplatzrechnern E-Mails. Jede eingehende, ausgehende oder interne E-Mail wird vom E-Mail-Server kopiert und an die EMA versandt und dort automatisch im Originalformat einem Hash-Verfahren unterzogen. Die EMA verschlüsselt alle archivierten E-Mails, sowohl auf der internen Festplatte, als auch dem externen Speicher. Auch von der verschlüsselten Datei wird der Hash-Wert gebildet. Sodann werden sowohl der verschlüsselte als auch der unverschlüsselte Hash-Wert über eine *Secure Sockets Layer* (SSL)-Verbindung mit Transportverschlüsselung an den von der ARTEC Computer GmbH betriebenen *Automated Network Administrator* (ANA)-Server versendet. Dieser versieht als vertrauenswürdiger Dritter die Hash-Werte mit einer sekundengenauen Zeit- und Datumsangabe und signiert dann den gesamten Datensatz mit einer fortgeschrittenen elektronischen Signatur.

Die archivierten E-Mails können auf einem oder mehreren externen Speichermedien abgelegt werden, auf die nur über die EMA zugegriffen werden kann. Die Nutzer können ihre empfangenen Nachrichten sowie Kopien der von ihnen versandten E-Mails zudem lokal in ihrem E-Mail-Client auf ihren Arbeitsplatzrechnern speichern. Auf das Archiv können sie nur von ihren Arbeitsplatzrechnern aus und nur nach einem Authentifizierungsverfahren unter Mitwirkung eines Authentifizierungsservers zugreifen.[1] Der Zugriff auf einzelne E-Mails oder deren Löschung können nur bei einer entsprechenden Berechtigung erfolgen, die von einem bei der archivierenden Stelle beschäftigten Administrator erteilt worden ist. Für die verschiedenen Aktivitäten des Administrators lässt sich eine Vier-Augen-Funktionalität aktivieren, sodass beispielsweise Zugriffe des Administrators auf Inhalte des Archivs nur unter Mitwirkung einer weiteren autorisierten Person möglich sind. Jeder Zugriff durch einen anderen als den jeweiligen Nutzer und jede Löschung wird im Archiv in einer Log-Datei protokolliert. Dies gilt auch für jedes Ein- oder Abschalten der Vier-Augen-Funktionalität. Die Protokolldaten werden ebenso wie die einzelnen E-Mails verschlüsselt und vom ANA-Server fortgeschritten signiert.

[1] Zum Authentifizierungsverfahren s. näher Abschnitt 2.2.1.

2 Wahrung des Daten- und Geheimnisschutzes

Die Archivierung der E-Mails mit EMA muss den Anforderungen des Daten- und Geheimnisschutzes entsprechen. Die E-Mails enthalten häufig personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse. Der bei der Archivierung erfolgende Umgang mit diesen Daten muss zum einen zulässig sein, zum anderen sind die personenbezogenen Daten sowie die Geheimnisse vor unbefugter Kenntnisnahme zu schützen.

2.1 Zulässigkeit der Speicherung von E-Mails

Die mithilfe von EMA archivierten E-Mails enthalten oft personenbezogene Daten im Sinn von § 3 Abs. 1 BDSG.[2] Die eingehenden und versendeten E-Mails werden kopiert und auf einem zentralen Speichermedium abgelegt. Die Speicherung ist eine Datenverarbeitung gemäß § 3 Abs. 4 Satz 1 BDSG. Die Verarbeitung personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Vielzahl von Anwendern ist aufgrund gesetzlicher Aufbewahrungspflichten zur Speicherung der von ihnen empfangenen und versandten E-Mails verpflichtet. Beispielsweise besteht für Kaufleute nach § 257 Abs. 1 Nr. 2 und 3 HGB und § 147 Abs. 1 Nr. 2 und 3 AO die Pflicht zur geordneten Aufbewahrung sowohl der empfangenen Handelsbriefe als auch von Wiedergaben der abgesandten Handelsbriefe. Zu den aufbewahrungspflichtigen Handelsbriefen gehören auch E-Mails.[3] Die meisten geschäftlichen E-Mails in Unternehmen unterliegen der Aufbewahrungspflicht und sind daher zu speichern.

Auch ohne eine gesetzliche Aufbewahrungspflicht ist die Speicherung personenbezogener Daten in vielen Fällen nach datenschutzrechtlichen Vorschriften zulässig. Die E-Mails können sowohl personenbezogene Daten des externen Kommunikationspartners als auch solche von Beschäftigten der aufbewahrenden Stelle enthalten. Hinsichtlich der Zulässigkeit der Datenspeicherung ist zwischen diesen beiden Arten personenbezogener Daten zu unterscheiden. Öffentliche Stellen können nach § 14 Abs. 1 Satz 1 BDSG oder den entsprechenden Vorschriften der Landesdatenschutzgesetze E-Mails mit personenbezogenen Daten ihrer Kommunikationspartner speichern, wenn dies zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist.

Soweit eingehende oder versendete E-Mails personenbezogene Daten über den externen Kommunikationspartner des Anwenders enthalten, ist deren Speicherung durch private Stellen oder öffentlich-rechtliche Wettbewerbsunternehmen in der Regel nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig, da sie der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Kommunikationspartner dient. Als vertragsähnliches Vertrauensverhältnis im Sinn der Vorschrift kommen zum Beispiel vertragliche Vorverhandlungen in Betracht.[4] Dient die Speicherung der E-Mails nicht einer der genannten Zweckbestimmungen, so kann sie gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Speicherung überwiegt. Ein berechtigtes Interesse liegt zum Beispiel vor, wenn das aufbewahrende Unternehmen die in den empfangenen E-Mails enthaltenen Kundendaten für Werbeaktionen nutzt, die es an die eigenen Kunden richtet. Im Einzelfall ist zu prüfen, ob die Speicherung der E-Mail für die Wahrung der berechtigten Interessen auch er-

---

[2] Dies könnte sich zwar durch eine Anonymisierung der Daten vermeiden lassen. Da die archivierten E-Mails dann aber ihre Informations- und Beweiszwecke nicht mehr erfüllen würden, wäre diese Maßnahme nicht sinnvoll.

[3] *Ballwieser*, in: MüKo-HGB, § 257 Rn. 12; *Cöster*, in: Pahlke/König 2004, § 147 Rn. 11.

[4] *Simitis*, in: ders. 2006, § 28 Rn. 121.

forderlich ist. Im Rahmen der Interessenabwägung ist zu berücksichtigen, dass der Absender die E-Mail an den Empfänger geschickt hat, um diesem in speicherbarer Textform bestimmte Informationen zukommen zu lassen. Ansonsten würde der Absender sich anderer Kommunikationsmedien bedienen. Der Empfänger darf daher grundsätzlich davon ausgehen, dass er mit der Aufbewahrung der E-Mails nicht gegen schutzwürdige Interessen des Absenders verstößt. Etwas anderes kann nur bei Vorliegen gegenteiliger Hinweise gelten.

Soweit E-Mails personenbezogene Daten der Beschäftigten der aufbewahrenden Stelle enthalten, sind für die Zulässigkeit der Speicherung die Mitbestimmungsrechte der Personalvertretung zu beachten. Nach § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Im öffentlichen Dienst unterliegen derartige Maßnahmen der Mitbestimmung des Personalrats gemäß § 75 Abs. 3 Nr. 17 BPersVG oder den entsprechenden Vorschriften der Landespersonalvertretungsgesetze. Die Zustimmung der Personalvertretung zu mitbestimmungspflichtigen Maßnahmen wird in der Regel im Rahmen einer Betriebsvereinbarung[5] nach § 77 BetrVG oder im öffentlichen Dienst im Rahmen einer Dienstvereinbarung[6] nach § 73 BPersVG oder den entsprechenden Vorschriften der Landespersonalvertretungsgesetze erklärt. Besteht bei der aufbewahrenden Stelle keine Personalvertretung, so ist die Speicherung der E-Mails nur zulässig, wenn sie gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG der Zweckbestimmung des zwischen der aufbewahrenden Stelle und dem Arbeitnehmer geschlossenen Arbeitsvertrags dient. Dies gilt nach § 12 Abs. 4 i.V.m. § 28 Abs. 1 Satz 1 Nr. 1 BDSG auch für personenbezogene Daten in den E-Mails von Beschäftigten öffentlicher Stellen.

Um zu beurteilen, ob die Speicherung der Zweckbestimmung des Arbeitsvertrags dient, bedarf es einer Unterscheidung zwischen den bei der aufbewahrenden Stelle eingehenden und den von ihr versendeten E-Mails. Eingehende dienstliche E-Mails sind an die aufbewahrende Stelle als Arbeitgeber gerichtet und werden von dem jeweiligen Arbeitnehmer lediglich für diese bearbeitet. Die Speicherung dieser E-Mails entspricht daher der Zweckbestimmung des Arbeitsvertrags. Ausgehende dienstliche E-Mails versendet der Arbeitnehmer im Namen des Arbeitgebers. Mithin dient auch die Speicherung dieser Nachrichten der Zweckbestimmung des Arbeitsvertrags und ist daher zulässig. Ob über die bloße Speicherung hinaus auch die Nutzung der in den E-Mails enthaltenen personenbezogenen Daten zur Bewertung und Kontrolle der Arbeitnehmer zulässig ist, richtet sich nach den Vorschriften des Arbeitnehmerdatenschutzrechts und eventueller Betriebs- oder Dienstvereinbarungen. Diese Vorschriften beschränken die Nutzungsmöglichkeit der Daten für den Arbeitgeber. Die EMA-Technik erlaubt die technisch-organisatorische Umsetzung solcher Beschränkungen, indem sie es ermöglicht, dass der Arbeitgeber auf die gespeicherten E-Mails aufgrund des Vier-Augen-Prinzips nur unter Mitwirkung des Betriebsrats oder des betrieblichen Datenschutzbeauftragten zugreifen kann.[7]

Für die Speicherung empfangener oder versendeter privater E-Mails durch den Arbeitgeber gibt es keinen Erlaubnistatbestand. Sollte der Arbeitgeber eine Differenzierung nach dienstlichen und privaten E-Mails vermeiden wollen, ist dies nur auf Basis einer Einwilligung der betroffenen Arbeitnehmer nach § 4a BDSG möglich.

---

5 *Büllesbach*, in: Roßnagel 2003, Kap. 6.1 Rn. 89.

6 *Hartig*, in: Roßnagel 2003, Kap. 6.2 Rn. 11.

7 S. hierzu ausführlich Abschnitt 2.2.1.5.

Ist die originäre Speicherung einer E-Mail nach § 28 Abs. 1 Satz 1 Nr. 1 oder 2 BDSG zulässig, so ist auch die Speicherung einer Sicherheitskopie in einem Archiv stets nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, da die aufbewahrende Stelle ein berechtigtes Interesse hat, ihre rechtmäßig entstandenen Datenbestände zum Zweck der Datensicherheit redundant zu speichern. Soweit dies durch entsprechende Schutzmaßnahmen für den Betroffenen keinen vertieften Grundrechtseingriff bedeutet, besteht auch kein Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Speicherung überwiegt. Die Sicherungskopien müssen einer strengen Zweckbindung unterliegen und gegen unbefugte Kenntnisnahme gesichert sein.[8]

Wenn ausnahmsweise keine gesetzliche Grundlage für die Speicherung der in den E-Mails enthaltenen personenbezogenen Daten besteht, darf sie nach § 4a Abs. 1 Satz 3 BDSG nur erfolgen, wenn der Betroffene eine wirksame Einwilligung hierfür abgegeben hat. Diese ist in Schriftform nach § 126 BGB zu erklären. Die Schriftform kann gemäß § 126 Abs. 3 BGB durch die in § 126a BGB definierte elektronische Form ersetzt werden.[9] Da die Speicherung der E-Mails, wie oben dargestellt, in den meisten Fällen aufgrund einer Rechtsvorschrift zulässig ist, wird die Einwilligung des Betroffenen in der Praxis nur von sehr geringer Relevanz sein.

Auch wenn die Speicherung von E-Mails mit personenbezogenen Daten zulässig ist, kann diese Zulässigkeit zeitlich begrenzt sein. Zum Beispiel beträgt die Aufbewahrungsfrist für Handelsbriefe gemäß § 257 Abs. 4 HGB und § 147 Abs. 3 Satz 1 AO sechs Jahre. Enthalten die Handelsbriefe personenbezogene Daten, so sind sie nach Ablauf der Aufbewahrungsfrist zu löschen, wenn eine längere Aufbewahrung nicht nach anderen Rechtsvorschriften oder aufgrund einer schriftlichen Einwilligung des Betroffenen zulässig ist. Ist die Speicherung der personenbezogenen Daten aus anderen Gründen als aufgrund einer Aufbewahrungspflicht zulässig, so sind die datenschutzrechtlichen Grundsätze der Zweckbindung und der Erforderlichkeit zu beachten.[10] Wenn der Zweck der Speicherung erreicht ist oder er nicht mehr erreicht werden kann, ist sie ab diesem Zeitpunkt unzulässig, sodass die Daten nach §§ 20 Abs. 2 und 35 Abs. 2 BDSG zu löschen sind. Die EMA-Technik erlaubt eine differenzierte Löschung von E-Mails und entspricht daher insoweit den Vorgaben des Datenschutzrechts. Bei den im Zusammenhang mit EMA verwendeten Speichermedien ist zu beachten, dass auch diese eine selektive Datenlöschung ermöglichen müssen.

2.2 Schutz vor unbefugter Kenntnisnahme

Bei der E-Mail Archivierung mit der EMA-Technik werden neben Betriebs- und Geschäftsgeheimnissen auch personenbezogene Daten automatisiert verarbeitet. Die aufbewahrende Stelle hat daher nach der Anlage zu § 9 Satz 1 BDSG ihre interne Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die Anlage sieht dabei verschiedene Anforderungen vor, die die Daten verarbeitende Stelle durch technisch-organisatorische Maßnahmen zu erfüllen hat. Die Maßnahmen müssen ausreichen, um die Funktion der jeweiligen Anforderungen aus dem Katalog der Anlage zu § 9 Satz 1 BDSG zu erfüllen. Die Anforderungen stehen jedoch nach § 9 Satz 2 BDSG unter dem Vorbehalt der Verhältnismäßigkeit, das heißt der Aufwand der Maßnahmen muss in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen. Soweit die Anforderungen gemäß der Anlage zu § 9 Satz 1 BDSG für die technische Gestaltung des Archivierungssystems relevant

---

8 S. hierzu die Ausführungen in Abschnitt 2.2.

9 *Simitis*, in: ders. 2006, § 4a Rn. 36.

10 S. hierzu *Roßnagel*, in: ders. 2003, Kap. 1 Rn. 41 ff.

sind, soll im Folgenden zunächst untersucht werden, ob die EMA-Technik zu ihrer vollständigen Erfüllung geeignet ist. Für den Fall, dass Defizite verbleiben, ist zu prüfen, ob die EMA-Technik unter Berücksichtigung des Verhältnismäßigkeitsvorbehalts den rechtlichen Anforderungen genügt.

2.2.1 Zugangs- und Zugriffsschutz

Insbesondere hat die Daten verarbeitende Stelle nach Nr. 2 der Anlage zu § 9 Satz 1 BDSG eine Zugangskontrolle zu gewährleisten, das heißt sie hat zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Darüber hinaus ist nach Nr. 3 der Anlage zu § 9 Satz 1 BDSG eine Zugriffskontrolle zu gewährleisten. Die aufbewahrende Stelle hat also sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zur Realisierung sowohl der Zugangs- als auch der Zugriffskontrolle bedarf es einer zuverlässigen Authentifizierung des Nutzers gegenüber dem Archivierungssystem. Zur Erfüllung dieser Anforderung sieht die EMA-Technik folgende Maßnahmen vor. Jeder Nutzer meldet sich zunächst mit seinem Benutzernamen und Passwort an seinem Arbeitsplatzrechner an. Für den darüber hinaus gehenden Zugriff auf seine mithilfe der EMA archivierten E-Mails bietet das System verschiedene Möglichkeiten an.

2.2.1.1 Anmeldung mittels Chipkarte und Passwort

Die EMA-Technik unterstützt die Anmeldung mittels Chipkarte. Dabei kann in der EMA eine Regel hinterlegt werden, welche Authentisierungszertifikate welcher Nutzer von der EMA akzeptiert werden. Der für das Authentisierungsverfahren notwendige private Schlüssel des Nutzers ist dabei auf dem Chip der Karte gespeichert und nicht auslesbar. Der Nutzer ruft die Web-Seite der EMA auf, führt seine Chipkarte in das Kartenlesegerät ein und aktiviert sodann den geheimen Schlüssel durch Eingabe eines Passworts. Der Zugriff auf die mit der EMA archivierten E-Mails ist bei diesem Verfahren an den Besitz der Karte und die Kenntnis des Passworts gebunden. Daher ist bei diesem Authentisierungsverfahren ein unberechtigter Zugriff durch bloßes Ausspähen des Passworts nicht möglich.

2.2.1.2 Einmalanmeldung (Single-Sign-On)

Alternativ zur Chipkarten-basierten Authentisierung lässt sich das Archivierungssystem so konfigurieren, dass ein Single–Sign-On-Verfahren zum Einsatz kommt. Hierbei authentisiert sich der Nutzer an seinem Arbeitsplatzrechner nur ein einziges Mal mit Benutzername und Passwort gegenüber dem Authentifizierungsserver. Danach erfolgt vor jedem Zugriff auf das Archiv eine automatische Identifikation des Nutzers durch das Single-Sign-On-System. Das von der EMA-Technik verwendete Verfahren wird durch das Kerberos-Authentifikationssystem unterstützt.[11] Dabei handelt es sich um einen Authentifikations- und Schlüsselaustauschdienst mit dessen Hilfe der Nutzer gegenüber einem Serverdienst – hier der EMA – authentifiziert wird, nachdem er sich zu Beginn seiner Sitzung am Arbeitsplatzrechner angemeldet hat. Erst nach erfolgreicher Authentifizierung kann der Nutzer auf seine im Archiv befindlichen E-Mails zugreifen. Auch ein Kopieren der E-Mails auf den Arbeits-

[11] S. ausführlich zum Kerberos-Authentifikationssystem *Eckert* 2006, 503 ff.

platzrechner des Nutzers ist nur nach ordnungsgemäßer Authentisierung des Nutzers gegenüber dem Archivierungssystem möglich.

Die Mitwirkung des Authentifizierungsservers verhindert, dass ein Angreifer sich von einem fremden Rechner aus ohne Weiteres gegenüber dem Archivierungsserver als berechtigter Nutzer ausgeben kann. Da das Passwort des Nutzers nicht über das Netz übertragen wird, kann das System auch nicht durch herkömmliche Phishing- oder Pharming-Angriffe auf das Passwort kompromittiert werden.

Obwohl das verwendete Kerberos-Authentifikationssystem somit einen erheblichen Fortschritt in Bezug auf die Sicherheit in offenen Netzen darstellt, ist es nicht frei von Defiziten.[12] Wer den Benutzernamen und das Passwort eines Nutzers kennt, kann sich von dessen Arbeitsplatzrechner aus erfolgreich über das Single-Sign-On-Verfahren bei der EMA anmelden. Nach einem erfolgreichen Offline-Angriff kann daher auch ein Unbefugter auf die E-Mails des Nutzers zugreifen. Dieses Risiko kann nur durch ein Smartcard-basiertes Challenge-Response-Verfahren ausgeräumt werden.

Eine weitere Schwachstelle des Kerberos-Verfahrens besteht darin, dass es für die gegenseitige Authentifizierung der beteiligten Rechner verschiedene Schlüssel verwendet, die auf dem Authentifizierungsserver ihrerseits mit einem Master-Key verschlüsselt und gespeichert werden. Der Master-Key ist ebenfalls auf der Festplatte des Authentifizierungsservers gespeichert und somit auslesbar. Um dies zu verhindern, muss der Master-Key auf einer unauslesbaren Smartcard gespeichert werden und die Verschlüsselung der anderen Schlüssel muss auf dem Chip der Karte stattfinden.

Anstatt des Kerberos-Verfahrens ist mit der EMA-Technik auch ein Single-Sign-On-Verfahren im Weg einer Challenge-Response-Authentifizierung nach dem *NT LAN Manager* (NTLM)-Standard möglich. Auch beim Einsatz dieses Verfahrens bleibt jedoch das Risiko eines Offline-Angriffs auf das Passwort bestehen, mit dem der Nutzer sich zu Beginn der Sitzung an seinem Arbeitsplatzrechner anmeldet.

Weitere Single-Sign-On-Verfahren, wie zum Beispiel die Anmeldung über eine Web-basierte Portallösung mit Hilfe eines SecurID-Tokens, lassen sich flexibel an die EMA anbinden. Zu diesem Zweck wird die Ticket-Server-Komponente der EMA innerhalb derselben Internet-Domäne installiert, in der die Anmeldung bereits durch ein etabliertes, Web-basiertes Single-Sign-On-Verfahren erfolgen kann. Mithilfe eines mit der EMA geteilten Schlüssels können das Authentifizierungsergebnis und die Identität des Nutzers sicher an die EMA weitergeben werden.

2.2.1.3 Anmeldung mittels Benutzername und Passwort

Für den Fall, dass das Single-Sign-On-Verfahren aufgrund der technischen Ausstattung des Nutzers nicht möglich ist, kommt auch eine Anmeldung über die Webseite des Archivierungsservers mit Benutzername und Passwort in Betracht. Die Webseite authentifiziert sich gegenüber dem Nutzer durch ein Verschlüsselungszertifikat. Die Zugehörigkeit des Zertifikats zum Archivierungsserver des Nutzers wird durch ein Zertifikat der ARTEC Computer GmbH bestätigt. durch die Authentisierung der Webseite werden Phishing-Angriffe auf das Passwort des Nutzers erschwert. Das Risiko eines unberechtigten Zugriffs nach einem erfolgreichen Offline-Angriff auf das Passwort bleibt indes bestehen.

[12] S. ausführlich zu den Defiziten von Kerberos *Eckert* 2006, 511 ff.

2.2.1.4 Verschlüsselung der E-Mails durch EMA

Die E-Mails werden von der EMA symmetrisch nach dem *Advanced Encryption Standard* (AES) verschlüsselt. Hierfür verwendet die EMA einen individuellen Schlüssel, der sich von den Schlüsseln anderer EMAs unterscheidet. Er ist so auf der EMA gespeichert, dass ein Zugriff auf ihn nicht möglich ist.

2.2.1.5 Zugriff des Systemadministrators

Neben dem jeweiligen Nutzer kann auch der Administrator des Archivierungssystems auf den gesamten Inhalt des Archivs zugreifen. Dies birgt grundsätzlich die Gefahr einer missbräuchlichen Kenntnisnahme von E-Mails einschließlich der darin enthaltenen personenbezogenen Daten. Die EMA-Technik ermöglicht zur Verhinderung dieser Gefahr die Einrichtung eines Vier-Augen-Prinzips. Wird dieses eingeschaltet, so kann der Administrator nur gemeinsam mit einer bestimmten anderen berechtigten Person, wie zum Beispiel einem Betriebsrat oder dem betrieblichen Datenschutzbeauftragten im Archiv nach E-Mails suchen und auf diese zugreifen. Das System ist zudem so gestaltet, dass auch das Einschalten und Abschalten des Vier-Augen-Prinzips durch den Administrator nur unter Mitwirkung mit einem anderen Berechtigten möglich ist. Jede derartige Änderung wird zudem in der Log-Datei protokolliert.

2.2.1.6 Protokollierung von Fremdzugriffen

Die gesetzlich geforderte Zugriffskontrolle erfolgt bei der EMA-Technik auch dadurch, dass die Zugriffe auf E-Mails in einer Log-Datei protokolliert werden. Dies gilt für die Zugriffe Dritter, wie etwa des Systemadministrators, nicht hingegen für Zugriffe des jeweiligen Nutzers, da seine E-Mails ohnehin auch auf seinem Arbeitsplatzrechner gespeichert sind, sodass er dort jederzeit darauf zugreifen kann. Die Protokolldaten werden verschlüsselt und ihr Hash-Wert sodann über eine SSL-Verbindung mit Transportverschlüsselung an den von der ARTEC Computer GmbH betriebenen ANA-Server versendet, der als vertrauenswürdiger Dritter die Protokolldaten in einem automatisierten Verfahren mit einer fortgeschrittenen elektronischen Signatur versieht. Die Signatur umfasst neben den Protokolldaten auch die Seriennummer der verwendeten EMA und den Signierzeitpunkt, der mithilfe der Systemzeit des ANA-Servers bestimmt wird. Durch die vorgenannten Maßnahmen lässt sich eine sehr weitreichende Zugriffskontrolle im Sinn von Nr. 3 der Anlage zu § 9 Satz 1 BDSG gewährleisten.

2.2.2 Weitergabekontrolle

Die Daten verarbeitende Stelle hat nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zu diesem Zweck kann die Kommunikation zwischen dem Arbeitsplatzrechner und dem Archivierungsserver über eine SSL-Verbindung mit Transportverschlüsselung erfolgen. Eine wirksame Weitergabekontrolle ist damit sichergestellt.

2.2.3 Eingabekontrolle

Nach Nr. 5 der Anlage zu § 9 Satz 1 BDSG hat die Daten verarbeitende Stelle zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Zum Schutz der archivierten E-Mails vor unbemerkten Veränderungen setzt die EMA-

Technik fortgeschrittene elektronische Signaturen gemäß § 2 Nr. 2 SigG ein. Die Kopien der empfangenen und versandten E-Mails werden zunächst noch vor deren Abruf durch den Nutzer beziehungsweise unmittelbar nach ihrer Versendung auf dem Archivierungsserver einem Hash-Verfahren unterzogen. Danach wird jede E-Mail verschlüsselt und auch von der so erzeugten Bit-Folge ein Hash-Wert gebildet. Beide Hash-Werte werden sodann an den als vertrauenswürdigen Dritten fungierenden ANA-Server versendet und dort fortgeschritten signiert. Die Signatur umfasst neben der archivierten E-Mail auch die Seriennummer der verwendeten EMA sowie die sekundengenaue Angabe des Zeitpunkts der Signaturerzeugung. Die von dem ANA-Server erzeugten Signaturen sind nur durch die EMA oder ein von der ARTEC Computer GmbH erhältliches Prüfprogramm prüfbar. Die signierten Hash-Werte werden zusammen mit der verschlüsselten E-Mail auf dem Archivierungsserver oder einem daran angeschlossenen Speichermedium gespeichert. Aufgrund der fortgeschrittenen Signatur lässt sich die verschlüsselte E-Mail nicht spurenlos verändern.[13]

Auch die Überprüfbarkeit der Eingabe von Daten ist wichtig, um feststellen zu können, ob E-Mails nachträglich in das Archiv eingefügt werden, die in Wahrheit nicht vom Arbeitsplatzrechner eines Nutzers aus verschickt worden sind. Ein Interesse an einer solchen Manipulation kann beispielsweise bestehen, wenn ein Beschäftigter der archivierenden Stelle es pflichtwidrig unterlassen hat, einem externen Geschäftspartner eine fristgebundene Nachricht zu schicken und dieses Fehlverhalten durch nachträgliches Einschmuggeln der Nachricht in das Archiv verschleiern will. Mithilfe des Zeitstempels des ANA-Servers lassen sich auch solche Manipulationen feststellen.

Zum Schutz der E-Mails vor einer unbemerkten Löschung wird jeder im Archiv vorgenommene Löschvorgang in einer Log-Datei protokolliert. Die Protokolldaten werden ihrerseits verschlüsselt und fortgeschritten signiert. Das System kann so konfiguriert werden, dass für die Ansicht und Auswertung der Protokolldaten der Zugriff von zwei verschiedenen autorisierten Personen gemäß dem Vier-Augen-Prinzip nötig ist. Die Feststellbarkeit einer unbefugten Dateneingabe, -veränderung oder -löschung ist aufgrund dieser Maßnahmen in hohem Maß gewährleistet.

2.2.4 Verfügbarkeitskontrolle

Die Daten verarbeitende Stelle hat nach Nr. 7 der Anlage zu § 9 Satz 1 BDSG zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Die für die E-Mail-Archivierung erforderliche Hardware und Software sind also vor Zerstörung durch zufällige Ereignisse wie Stromausfälle, Wassereinbrüche oder Blitzschläge zu schützen. Zur Vermeidung von Blitzschlägen genügen zum Beispiel die Einrichtung eines besonders abgesicherten Stromanschlusses und die galvanische Trennung von Netzwerkanschlüssen.[14] Der Gefahr von Stromausfällen kann mit einer unterbrechungsfreien Stromversorgung begegnet werden. Dabei wird in der Regel der Stromausfall für einen begrenzten Zeitraum mit Batteriepufferungen überbrückt. In dieser Zeit kann mithilfe einer entsprechenden Software das Datenverarbeitungssystem automatisch und ordnungsgemäß beendet und abgeschaltet und auf diese Weise können Hardwareschäden oder Datenverluste vermieden werden. Diese Maßnahmen lassen sich mit dem Betrieb der EMA-Technik ohne Schwierigkeiten vereinbaren, so dass die EMA insoweit den rechtlichen Vorgaben entspricht.

---

[13] Ausführlich zum Integritätsschutz durch fortgeschrittene elektronische Signaturen s. *Roßnagel*, MMR 2003, 164 ff.

[14] *Ernestus*, in: Simitis 2006, § 9 Rn. 156.

Jede E-Mail wird sofort bei ihrem Eingang auf dem Archivierungsserver auf ein oder mehrere externe Speichermedien kopiert. Dies gilt auch für sämtliche Protokolldaten. Daher ist selbst bei Verlust der EMA der Schutz des gesamten Archivs vor zufälligem Datenverlust gewährleistet. Zwar wären in diesem Fall die verschlüsselten Archivdaten zunächst nicht lesbar, da der zur Entschlüsselung benötigte individuelle Schlüssel in der EMA gespeichert ist. Die ARTEC Computer GmbH kann aber ein Austauschgerät zu Verfügung stellen, das den Schlüssel der alten EMA enthält, sodass die Entschlüsselung und damit auch die Lesbarmachung der Daten möglich bleibt.

Schließlich wird die Verfügbarkeit der Daten auch durch die von der EMA vorgenommene Konsistenzprüfung gesichert. Dabei erfolgt in regelmäßigen, von der archivierenden Stelle definierten Abständen ein automatisierter Abgleich aller auf dem externen Speichermedium gespeicherten Archivinhalte mit den Daten, die im Cache der EMA und falls vorhanden auf weiteren externen Speichern abgelegt sind. Falls einzelne Dateien defekt sind, stellt die EMA sie automatisch wieder her. Im Rahmen dieses Verfahrens werden auch die elektronischen Signaturen geprüft und die archivierende Stelle per E-Mail über fehlgeschlagene Prüfungen unterrichtet. Die Konsistenzprüfung und die rechtzeitige Wiederherstellung der Daten ermöglichen es, die Verfügbarkeit der Archivinhalte zu gewährleisten.

2.2.5 Technisch-organisatorische Realisierung der Zweckbindung

Nach Nr. 8 der Anlage zu § 9 Satz 1 BDSG ist sicherzustellen, dass zu unterschiedlichen Zwecken gespeicherte Daten getrennt verarbeitet werden können. In diesem Zusammenhang ist insbesondere zu berücksichtigen, dass für Daten, die zu unterschiedlichen Zwecken gespeichert wurden, verschiedene Speicherfristen gelten können. Daher ist zu gewährleisten, dass ein autorisierter Nutzer jederzeit einzelne E-Mails aus dem Archiv löschen kann. Dies ist bei der EMA-Technik der Fall. Zur Nachvollziehbarkeit dieses Vorgangs wird die Löschung protokolliert. Die Anforderung aus Nr. 8 der Anlage zu § 9 Satz 1 BDSG ist damit erfüllt.

2.2.6 Erforderlichkeit der technisch-organisatorischen Maßnahmen

Wie die bisherigen Ausführungen zeigen, wird die EMA-Technik den besonderen Anforderungen des Datenschutzes im Sinn der Anlage zu § 9 Satz 1 BDSG in hohem Maß gerecht. Die Beseitigung der verbleibenden technisch-organisatorischen Defizite ist jedoch nach § 9 Satz 2 BDSG nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Bei dem angestrebten Schutzzweck geht es darum, den unzulässigen Umgang mit personenbezogenen Daten zu verhindern und die Richtigkeit der Daten während der gesamten Aufbewahrungszeit sicherzustellen.[15] Bei der Gewichtung des Schutzzwecks im Rahmen der nach § 9 Satz 2 BDSG vorzunehmenden Abwägung ist überdies der Grad der Sensitivität der gespeicherten Daten zu berücksichtigen und als Folge davon der Schaden einer hypothetischen Beeinträchtigung des Betroffenen im Fall eines unberechtigten Datenzugriffs. Weiterhin ist die Wahrscheinlichkeit einer Beeinträchtigung zu beachten.[16] Der mit den technischen Maßnahmen angestrebte Schutzzweck lässt sich somit nicht allgemein, sondern nur in Bezug auf eine konkrete Anwendung, also unter Berücksichtigung der im Einzelfall tätigen archivierenden Stelle bestimmen. Er ist mit dem Aufwand optimierter technisch-organisatorischer Maßnahmen unter Berücksichtigung der hierfür anfallenden Kosten abzuwägen. Auch diese Abwägung kann nur in Kenntnis der konkreten Umstände des jeweiligen Einzelfalls erfolgen.

---

[15] *Ernestus*, in: Simitis 2006, § 9 Rn. 26.

[16] *Ernestus*, in: Simitis 2006, § 9 Rn. 27.

Die EMA-Technik gewährleistet jedoch eine Datensicherheit, deren Grad weit über dem Durchschnitt dessen liegt, was die Sicherheitsmaßnahmen Daten verarbeitender Stellen in der Praxis leisten. Die Sicherheit der EMA-Technik reicht daher für die meisten Anwendungsbereiche aus. Die Sicherheit des Archivsystems hängt auch von der technischen Einsatzumgebung der EMA, insbesondere von dem verwendeten Authentifizierungssystem ab. Auch bei dessen Auswahl müssen mithin das Ausmaß und die Wahrscheinlichkeit der hypothetischen Beeinträchtigung des Betroffenen berücksichtigt werden. Für einzelne Anwendungsfelder, wie zum Beispiel besondere medizinische Anwendungen ist daher bei Abwägung der Schutzwecks der Verhinderung unbefugter Kenntnisnahme mit dem zur Optimierung der Datensicherheit notwendigen Aufwand ein besonders hohes Maß an Sicherheit, wie etwa durch den Einsatz von Chipkarten-basierten Systemen, erforderlich.

3 Erfüllung von Aufbewahrungspflichten

Soweit die archivierende Stelle zur Aufbewahrung ihrer E-Mails verpflichtet ist, muss die Verwendung der EMA-Technik auch den rechtlichen Anforderungen an eine rechtssichere Aufbewahrung genügen. Die Einzelheiten zu den bereichsspezifischen Aufbewahrungspflichten sind in verschiedenen für die jeweiligen Anwendungsbereiche geltenden Vorschriften geregelt, die zwischen unterschiedlichen Dokumentenarten differenzieren. Unabhängig vom konkreten Anwendungsbereich gibt es indes Grundanforderungen, die stets für die Aufbewahrung von Dokumenten gelten. Hierzu gehören zunächst die Lesbarkeit, die Integrität und die Authentizität der aufzubewahrenden Dokumente.[17]

Die Lesbarkeit erfordert, dass die in den aufbewahrten E-Mails enthaltenen Informationen jederzeit sichtbar gemacht werden können. Elektronische Dokumente sind nur dann lesbar, wenn sie in einem Datenformat vorliegen, das mit Hilfe der jeweils zur Verfügung stehenden Hard- und Software verarbeitet werden kann. Die in den Dokumenten enthaltenen Informationen müssen interpretiert und dem menschlichen Betrachter in lesbarer Weise präsentiert werden können. Zu diesem Zweck werden die E-Mails bei Verwendung der EMA nicht konvertiert, sondern im bereits seit 1982 existierenden Originalformat RFC 822 gespeichert. Es ist nicht zu erwarten, dass dieses Format in absehbarer Zeit abgelöst wird. Die archivierten E-Mails können daher langfristig lesbar gemacht werden.

Neben der Lesbarkeit sind auch die Integrität und die Authentizität der archivierten E-Mails sicherzustellen. Dabei wird unter dem Begriff der Integrität die Unversehrtheit der archivierten Daten verstanden, während mit der Authentizität die eindeutige Bestimmbarkeit des Verfassers einer E-Mail gemeint ist. Inwieweit die EMA-Technik die Integrität und die Authentizität der aufbewahrten Dokumente gewährleistet, wird im Abschnitt zum Beweiswert der archivierten E-Mails untersucht.[18]

Für den Fall, dass nicht nur die Aufbewahrung einzelner Dokumente, sondern die die Dokumentation eines zusammenhängenden Vorgangs von Bedeutung ist, und daher die Gesamtzusammenhang einer Vielzahl von Dokumenten erhalten bleiben muss, ist die Vollständigkeit der zu dem Vorgang gehörenden E-Mails zu gewährleisten.[19] Die EMA-Technik ermöglicht dies dadurch, dass die Löschung einzelner Dokumente stets in den Protokolldaten vermerkt

---

[17] S. hierzu ausführlich *Roßnagel/Fischer-Dieskau/Jandt/Knopp* 2007, 43 ff.; *Roßnagel/Fischer-Dieskau/Jandt* 2007, 15f.

[18] S. unten Abschnitt 4.2.

[19] *Roßnagel/Fischer-Dieskau/Jandt/Knopp* 2007, 100.

wird und diese durch die Verschlüsselung und die Signatur des ANA-Servers vor einer Manipulation geschützt werden. Zwar besteht die Möglichkeit, dass der Nutzer einzelne zu einem Vorgang gehörende E-Mails zwecks Umgehung des Archivs nicht von seinem Arbeitsplatzrechner, sondern von einem fremden Rechner unter Nutzung eines privaten E-Mail-Accounts versendet. Technische Möglichkeiten zur Verhinderung eines solchen Vorgangs bestehen jedoch nicht. Die EMA-Technik ist somit nach dem gegenwärtigen Stand der Technik zur Gewährleistung der Vollständigkeit der zu einem Vorgang gehörenden E-Mails geeignet.

Schließlich muss das Archivierungssystem die Verkehrsfähigkeit der archivierten E-Mails sicherstellen, also die Möglichkeit, die E-Mails von einem technischen System so in ein anderes zu übertragen, dass ihre Integrität und Authentizität nachweisbar bleiben.[20] Auch auf die Verkehrsfähigkeit der mit der EMA-Technik archivierten Dokumente wird in den Ausführungen zum Beweiswert näher eingegangen.[21]

4 Beweiswert der archivierten E-Mails

Die Archivierung von E-Mails dient neben der Funktionsfähigkeit der archivierenden Stelle und der Erfüllung von Aufbewahrungspflichten im Interesse von Einsichts- und Kontrollberechtigten auch den Beweisführungsinteressen der archivierenden Stelle und Dritter.[22] Im Folgenden soll der Beweiswert der mithilfe der EMA-Technik archivierten E-Mails untersucht werden.

4.1 Anwendung der Vorschriften über den Urkundsbeweis

Nach geltendem Beweisrecht ist eine Behauptung bewiesen, wenn das Gericht nach dem Grundsatz der freien Beweiswürdigung gemäß § 286 Abs. 1 Satz 1 ZPO von ihrer Wahrheit überzeugt ist.[23] Dabei genügt ein für das praktische Leben brauchbarer Grad an Gewissheit, da es eine absolute Sicherheit nicht gibt.[24] Eine Ausnahme von diesem Grundsatz besteht nach § 286 Abs. 2 ZPO nur dort, wo das Gesetz ausdrückliche für das Gericht bindende Beweisregeln vorsieht, um bestimmte Beweismittel im Interesse der Beweissicherheit zu unterstützen oder den Beweisführer von bestimmten Beweisrisiken zu entlasten. Solche Regeln kennt das Recht zum Beispiel für öffentliche und private Urkunden in §§ 415 ff. ZPO.[25] Nach § 416 ZPO begründen Privaturkunden vollen Beweis für die Abgabe der in ihnen enthaltenen Erklärungen. Nach §§ 415, 417 und 418 ZPO gilt für öffentliche Urkunden, dass sie vollen Beweis für den beurkundeten Vorgang, für amtliche Anordnungen, Verfügungen und Entscheidungen sowie für die in ihnen bezeugten Tatsachen begründen.

Da elektronische Dokumente nicht ohne technische Hilfsmittel wahrnehmbar sind, stellen sie keine Urkunden im Sinn des Beweisrechts dar, sondern sind als Objekte des Augenscheins in den Prozess einzubringen.[26] Die Vorschriften der §§ 415 ff. ZPO sind daher auf sie nicht un-

---

[20] *Roßnagel/Fischer-Dieskau/Jandt* 2007, 16.

[21] S. unten Abschnitt 4.3.

[22] S. ausführlich zum Zweck der Aufbewahrung von Dokumenten *Roßnagel/Fischer-Dieskau/Jandt/Knopp* 2007, 35 ff.

[23] Zum Beweiswert elektronischer Dokumente s. eingehend *Roßnagel/Wilke*, NJW 2006, 2147. Da die meisten Verfahrensordnungen für die Beweisregelungen auf die ZPO verweisen (§ 173 VwGO, § 155 FGO, § 202 SGG, § 46 Abs. 2 ArbGG), wird im Folgenden nur auf die Regeln der ZPO eingegangen.

[24] *BGH*, NJW 1993, 935.

[25] Öffentliche Urkunden sind solche, die von einer öffentlichen Stelle, wie z.B. einer Behörde, einem Gericht oder einem Notar ausgestellt sind.

[26] *Huber*, in: Musielak 2008, § 415 Rn. 5 m.w.N.

mittelbar anwendbar. Der Gesetzgeber sieht jedoch in § 371a Abs. 1 Satz 2 ZPO eine Beweiserleichterung für private elektronische Dokumente vor, wenn sie mit einer qualifizierten elektronischen Signatur versehen sind. Für die Echtheit dieser Dokumente gilt ein vorweggenommener Anscheinsbeweis. Für öffentliche Dokumente verstärkt § 371a Abs. 2 Satz 1 ZPO diese Vermutungswirkung, indem er die entsprechende Anwendung der Vorschriften über die Beweiskraft öffentlicher Urkunden anordnet.

Soweit die mithilfe der EMA-Technik archivierten E-Mails mit einer qualifizierten elektronischen Signatur versehen sind, bewahrt das Archivierungssystem auch die Signatur im Originalformat auf, sodass sie prüfbar bleibt. Nach § 371a i.V.m. §§ 415 ff. ZPO haben sie also dieselbe Beweiskraft wie Papierurkunden.

4.2 Freie Beweiswürdigung

Archivierte E-Mails ohne qualifizierte elektronische Signatur sind Gegenstand der freien richterlichen Beweiswürdigung. Der Richter entscheidet also im Wesentlichen frei darüber, welchen Beweiswert er ihnen zumisst. Er muss bei seiner Entscheidungsfindung aber die Denkgesetze, die zwingenden Erfahrungssätze und die Naturgesetze beachten.[27] Ist eine vom Verfasser nicht signierte E-Mail Beweismittel für eine beweiserhebliche Tatsache, so hat der Beweisführer im Gerichtsverfahren gute Erfolgsaussichten, wenn er den Richter davon überzeugen kann, dass die E-Mail nach ihrer Absendung nicht verändert worden ist (Integrität), und dass sie tatsächlich von dem Aussteller herrührt, von dem sie zu stammen scheint (Authentizität).

4.2.1 Integritätsnachweis

Für den Integritätsnachweis der E-Mails ist zwischen der Zeit vor und nach dem Eingang in das Archivierungssystem zu differenzieren. Für eine von außen kommende E-Mail gilt, dass sie vor ihrem Eingang ins Archiv abgefangen und in Ermangelung einer Signatur unbemerkt verändert werden kann.[28] Eine vom Nutzer versendete E-Mail ist im Zeitraum vor ihrem Eingang ins Archiv allenfalls einem äußerst geringen Angriffsrisiko ausgesetzt, da sie unmittelbar nach der Absendung vom Arbeitsplatzrechner auf dem E-Mail-Server des Nutzers kopiert und die Kopie an die EMA gesandt und im Archiv abgelegt wird.

Die Integrität der im Archivierungssystem eingegangenen E-Mails ist im Prozess nachweisbar, wenn nachträglich überprüft und festgestellt werden kann, ob und von wem die archivierten E-Mails verändert oder entfernt worden sind. Den Schutz der Integrität bestimmen dieselben Maßnahmen, die auch zur Gewährleistung der Datensicherheit, insbesondere der Eingabekontrolle nach Nr. 5 der Anlage zu § 9 Satz 1 BDSG durchgeführt werden.[29] Insoweit bietet das Archivierungssystem eine hohe Datensicherheit, die auch den Beweiswert der archivierten E-Mails erhöht. Neben diesem systembezogenen Integritätsschutz lässt sich die Unveränderheit der archivierten E-Mails aufgrund der fortgeschrittenen elektronischen Signaturen des ANA-Servers jederzeit dokumentbezogen mathematisch nachweisen.

Der Zeitraum des Eingangs der E-Mails in das Archiv lässt sich mithilfe des Zeitstempels des ANA-Servers nachvollziehen. Der Umstand, dass dieser als vertrauenswürdiger Dritter den Beginn der Archivierung bestimmt, erleichtert es dem Gericht, die Wahrscheinlichkeit einer

---

[27] *Prütting*, in: MüKo-ZPO, § 286 Rn. 10.

[28] Ausführlich zu dieser Problematik *Roßnagel/Pfitzmann*, NJW 2003, 1210.

[29] S. hierzu oben Abschnitt 2.2.3.

Manipulation einer an den Nutzer adressierten E-Mail vor ihrem Eingang ins Archiv einzuschätzen. Von einer Manipulation einer E-Mail kann allenfalls dann ausgegangen werden, wenn ein Manipulationsinteresse einer Partei schon vor dem Eingang ins Archiv bestanden haben kann.

4.2.2 Authentizitätsnachweis

Ebenso wie die Integrität der von außen eingehenden unsignierten E-Mails ist auch deren Authentizität nicht durch Archivierungsmaßnahmen des Empfängers sicherzustellen, denn ein Angreifer kann seine Nachrichten unter einer fremden E-Mail-Adresse versenden.[30] Weniger wahrscheinlich ist, dass dem Archivsystem E-Mails untergeschoben werden, die entgegen dem durch ihre Absenderadresse erzeugten Anschein in Wahrheit nicht vom Nutzer stammen. Auch dies ist aber möglich, wenn ein Angreifer sich nach erfolgreichem Offline-Angriff mit dem Benutzernamen und dem Passwort des Nutzers am Rechnersystem anmeldet.

4.3 Verkehrsfähigkeit der archivierten E-Mails

Nach § 371 Abs. 1 Satz 2 ZPO wird der Beweis mit elektronischen Dokumenten durch Vorlegung oder Übermittlung der Datei an das Gericht angetreten. Die im Archivsystem gespeicherten E-Mails lassen sich ohne Weiteres elektronisch an das Gericht übermitteln. Der Beweis dafür, dass die E-Mails während des Archivierungszeitraums nicht verändert worden sind, wird durch die Protokolldaten der EMA erbracht, die dem Gericht ebenfalls elektronisch übermittelt werden können. Mithilfe der Signaturen des ANA-Servers, die auch die Seriennummer der verwendeten EMA enthalten, wird lässt sich der Nachweis erbringen, dass die E-Mail in dem Archivsystem aufbewahrt wurde, auf das sich die beigebrachten Protokolldaten beziehen. Ein Rückgriff auf die beim Nutzer befindliche Hardware ist daher für die Beweisführung nicht erforderlich.

5 Ergebnis

Die EMA-Technik ist für eine rechtssichere Archivierung von E-Mails in hohem Maß geeignet. Die angewendeten Maßnahmen zur Gewährleistung der Datensicherheit liegen über dem Durchschnitt der heutigen Praxis Daten verarbeitender Stellen und reichen für die meisten Anwendungsbereiche aus. Die im Rahmen von Aufbewahrungspflichten anwendungsübergreifend geltenden Anforderungen sind mit der EMA-Technik erfüllbar. Die auf diese Weise archivierten E-Mails haben einen hohen Beweiswert. Zwar kann die EMA keinen Schutz davor bieten, dass von außen eingehende E-Mails vor ihrem Eingang ins Archiv abgefangen und manipuliert werden. Ab diesem Zeitpunkt gewährleistet sie jedoch eine hohe Beweissicherheit. Dies beruht zum einen auf der systembezogenen Sicherheit vor unbemerkten manipulierenden Zugriffen auf das Archiv sowie zum anderen auf der dokumentenbezogenen Sicherheit, die mit den fortgeschrittenen elektronischen Signaturen des als vertrauenswürdigen Dritten fungierenden ANA-Servers erzielt wird. Die Signaturen ermöglichen einen jederzeitigen mathematischen Nachweis der Unversehrtheit, an den die Gerichte im Rahmen der freien Beweiswürdigung gebunden sind.

Hinsichtlich des Nachweises der Authentizität der archivierten E-Mails ist festzustellen: Für ausgehende E-Mails des Nutzers bietet die EMA-Technik aufgrund des verwendeten Authentifizierungsverfahrens in der Regel ausreichende Anhaltspunkte, die im Rahmen der freien Beweiswürdigung bei der Beurteilung der Authentizität der E-Mail zu einem positiven Er-

[30] S. hierzu ausführlich *Roßnagel/Pfitzmann*, NJW 2003, 1210f.

gebnis führen dürften. Für von außen eingehende E-Mails ist die Zeit vor und nach ihrer Archivierung zu unterscheiden: Für die Zeit vor der Archivierung könnte aufgrund der Unsicherheit von E-Mail-Verfahren ein Authentizitätsnachweis nur geführt werden, wenn die Mails mit einer dokumentbezogenen Sicherung in Form einer qualifizierten Signatur versehen wären. Ob der Absender seine E-Mails signiert, kann die archivierende Stelle jedoch nicht durch technisch-organisatorische Maßnahmen beeinflussen. Der „Verantwortungsbereich“ der der EMA-Technik beginnt jedoch erst ab der Archivierung. Für diese erfüllt die EMA-Technik die rechtlichen Anforderungen.

Literatur

Eckert, C., IT-Sicherheit: Konzepte – Verfahren – Protokolle, 4. Auflage, München 2006.

Münchener Kommentar zum Handelsgesetzbuch, Schmidt, K. (Hrsg.), Band 4: Drittes Buch. Handelsbücher, §§ 238-342e HGB, 2. Auflage, München 2008 (zitiert als: *Bearbeiter*, in: MüKo-HGB).

Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, Rauscher, T. / Wax, P. / Wenzel, J. (Hrsg.), Band 1: Einleitung, §§ 1-510c, 3. Auflage, München 2008 (zitiert als: *Bearbeiter*, in: MüKo-ZPO).

Musielak, H.-J. (Hrsg.), Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz, 6. Auflage, München 2008.

Pahlke, A. / Koenig, U. (Hrsg.), Abgabenordnung – §§ 1 bis 368 – Kommentar, München 2004.

Roßnagel, A., Die fortgeschrittene elektronische Signatur, MMR 2003, 164.

Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Roßnagel., A. / Fischer-Dieskau, S. / Jandt, S., Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, BMWi-Dokumentation Nr. 564, Wernigerode 2007.

Roßnagel., A. / Fischer-Dieskau, S. / Jandt, S. / Knopp, M., Langfristige Aufbewahrung elektronischer Dokumente – Anforderungen und Trends, Baden-Baden 2007.

Roßnagel, A. / Pfitzmann, A., Der Beweiswert von E-Mail, NJW 2003, 1209.

Roßnagel, A. / Wilke, D., Die rechtliche Bedeutung gescannter Dokumente, NJW 2006, 2145.

Simitis, S. (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006.

Abkürzungen

Abs.	Absatz
AES	Advanced Encryption Standard
ANA	Automated Network Administrator
AO	Abgabenordnung
ArbGG	Arbeitsgerichtsgesetz
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGH	Bundesgerichtshof
BMWi	Bundesministerium für Wirtschaft und Technologie
BPersVG	Bundespersonalvertretungsgesetz
ders.	derselbe
EMA	E-Mail Archive Appliance
FGO	Finanzgerichtsordnung
Fn.	Fußnote
GmbH	Gesellschaft mit beschränkter Haftung
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
Kap.	Kapitel
LAN	Local Area Network
MMR	Multimedia und Recht
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NTLM	NT LAN Manager
Rn.	Randnummer
s.	siehe
SGG	Sozialgerichtsgesetz
SigG	Signaturgesetz
SSL	Secure Sockets Layer
VwGO	Verwaltungsgerichtsordnung
z.B.	zum Beispiel
ZPO	Zivilprozessordnung