Sicherheitsrisiken beim Rechnungsversand per Email

Printout von blog.jakobs.systems

Tomas Jakobs

06.08.2025

Inhaltsverzeichnis

Anfang des Jahres sorgte ein Urteil des Schleswig-Holsteinischen Oberlandesgerichts (Az. 12 U 9/24) für Aufmerksamkeit in Blogs und Newstickern. Aus diesem geht hervor, dass Unternehmen schadensersatzpflichtig werden, sollten sie ohne Sicherheitsmaßnahmen Ihre Rechnungen unverschlüsselt per Email verschicken und es in Folge zu einer Manipulation und Überweisung an unberechtigte Dritte kommt.[1]

Grundlage des Verfahrens war, dass der Anhang einer E-Mail, genauer eine Rechnung im PDF-Format, verändert wurde. Die Manipulation war eine Änderung der IBAN des rechnungausstellenden Unternehmens.

Das vorherige Landgericht Kiel stellte fest, die Überweisung einer Abschlags- und zugleich Abschlußrechnung eines Werkvertrages in Höhe von 15.385,78 EUR (skonto-gemindert 14.924,20) auf ein “untergeschobenes” Konto eines Dritten stellt keine Erfüllung der Forderung dar. Der Kunde, ein anderes Unternehmen, muss die Rechnung erneut auf das richtige Konto begleichen. Soweit zu den Grundlagen des BGB.

Schadensersatzanspruch wegen DSGVO-Verstoß

Interessant wird es bei der eingelegten Berufung des betroffenen Unternehmens. Dieses machte Schadensersatzanspruch in Höhe der getätigten Überweisung geltend. Der Anspruch ergibt sich aus dem Arglisteinwand[2] gem. §242 BGB.[3] Das Unternehmen handelte in Treu und Glauben und könne nichts für die Manipulation der per Email zugegangenen PDF-Rechnung.

Das OLG Schleswig stellte im Urteil darauf ab, dass der unverschlüsselte Versand ein Verstoß gegen Artikel 32 DSGVO[4] sei. Es handele sich um eine Verarbeitung im Sinne von Artikel 4 DSGVO[5], nämlich der Offenlegung durch Übermittlung. Das rechnungserstellende Unternehmen habe keine hinreichende Sicherheitsmaßnahmen getroffen und müsse daher für den entstandenen Schaden vollumfänglich aufkommen. Im Volltext heißt es:[6]

---

[1] https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/OLG/Presse/PI/202501Werklohnrechnung

[2] https://de.wikipedia.org/wiki/Dolo_agit

[3] https://www.gesetze-im-internet.de/bgb/__242.html

[4] https://dejure.org/gesetze/DSGVO/32.html

[5] https://dejure.org/gesetze/DSGVO/4.html

[6] https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/OLG/Presse/PI/202501Werklohnrechnung

> Eine reine Transportverschlüsselung beim Versand von geschäftlichen E-Mails … zwischen Unternehmer und Kunden … bei dem hier bestehenden hohen finanziellen Risiko durch Verfälschung der angehängten Rechnung … (ist) nicht ausreichend und kann keinen "geeigneten" Schutz im Sinne der DSGVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl.

Ohne auf die tatsächlichen Ursachen und kausalen Zusammenhänge einzugehen geht das OLG von einem "Man in the Middle" Angriff[7] aus.

Zuvor stellte das Landgericht Kiel lediglich fest, dass eine Mail mit der Originalrechnung vom Absender versandt und eine Mail mit manipulierter Rechnung im Posteingang des Empfängers einging.

Bewertung

Vertraulichkeit, Authentizität und Integrität einer Nachricht ist nur durch eine End-to-End Verschlüsselung gewährleistet. So weit richtig. In der praktischen Anwendung ist das jedoch die ultima ratio, der Hammer im IT-Werkzeugkasten mit Nebenwirkungen und anderen Risiken, die abzuwägen sind.

Risikobasierte Abwägungen ziehen sich wie ein roter Faden durch die DSGVO. Das findet hier aber keine Berücksichtigung. Im vorliegenden OLG Urteil klafft die "offene Flanke", dass von den persönlichen Daten auf der gegenständlichen Rechnung es ausgerechnet die von der DSGVO nicht erfasste IBAN ist, die hier manipuliert wurde und zur Fehlüberweisung führte. Der kausale Zusammenhang zwischen DSGVO-Verletzung und entstandenem Schaden fehlt, so die Beck'sche Kommentierung.[8]

Die Manipulation der PDF-Rechnung durch einen "Man in the Middle" Angriff hätte beispielsweise auch mit Hilfe einer lediglich signierten Email verhindert werden können.

Es bleibt dahingestellt, auf welcher Seite und ob überhaupt ein technisches System kompromittiert wurde. Im Raum stehen auch möglicherweise strafrechtliche Vergehen der betroffenen Mitarbeiter, die eine manipulierte Rechnung in den Rechnungsprozess einbrachten.

---

[7] https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff

[8] https://beck-online.beck.de/Bcid/Y-300-Z-ZD-B-2025-S-284-N-1

Einmal in den Raum geworfen: Sind die Absender- und Empfängerdaten nicht meist hinter einem Klarsichtfenster auch auf einem klassichen Briefumschlag für jeden mitlesbar?

In Hinblick auf die unvollständigen Feststellungen und offen gebliebene Kausalität, bleibt es spannend, ob und wie dieses Urteil künftig zitiert wird.

Risikobasierte Sicherheitsmaßnahmen

Im Folgenden eine Übersicht möglicher technischer Schutzmaßnahmen ohne Anspruch auf Vollständigkeit oder Allgemeingültigkeit:

Signierte Emails mit S/MIME oder PGP Zum Signieren von Emails zusammen mit Ihren Anlagen gibt es im Internet zwei RFC-standardisierte Verfahren:

S/MIME (Secure/Multipurpose Internet Mail Extensions)[9] nutzt öffentliche, von Dritten beglaubigte Zertifikate, die meist kostenpflichtig zu beziehen sind. Die Straßenpreise für emailvalidierende Zertifikate beginnen bei 19,- EUR p.a. Darüber hinaus gibt es identitätsvalidierende und organisationsvalidierende Zertifikate, mit strengeren Prüfungen und höheren Kosten.

(Open)PGP (Pretty Good Privacy)[10] ist von der funktionsweise ähnlich, nutzt jedoch selbst erstellte Schlüsselpaare ohne eine validierende Zertifikatsstelle. Eine Verschlüsselung hier erfordert einen manuellen Schlüsselaustausch. Signierte Nachrichten können jedoch auch ohne Schlüsseltausch zumindest gelesen werden.

Ich muss nicht erwähnen, dass Windows von Haus nicht mit den allgemeinen Internetstandards umgehen kann und die entsprechenden Tools fehlen. Hier muss die Software gpg4win mit Ihren cross-compilierten Tools installiert werden.[11] Wer den Mozilla Thunderbird unter Windows nutzt, braucht diese zusätzlichen Software nicht.[12]

Beide Verfahren haben ihre Vor- und Nachteile. S/MIME ist in Unternehmen etwas weiter verbreitet und wird von den typischen Email-Clienten wie Outlook nativ unterstützt, gilt aber

[9] https://de.wikipedia.org/wiki/S/MIME

[10] https://de.wikipedia.org/wiki/OpenPGP

[11] https://gpg4win.org/

[12] https://thunderbird.net/de/

seit den E-Fail Aufdeckungen als unsicherer.[13]

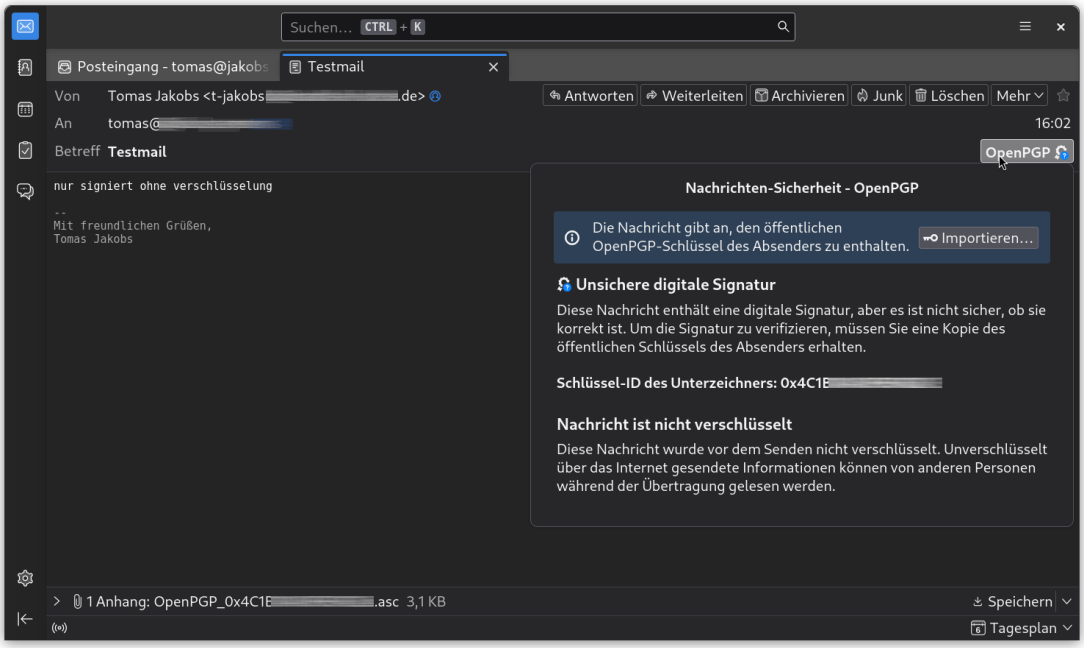

Abbildung 1: Screenshot Thunderbird mit einer signierten Email

Signierte Dateien Fehlt die Akzeptanz bei den Mitarbeitern, die Unterstützung im Email-Clienten oder werden Rechnungen automatisiert ohne Benutzerinteraktion einem Dokumentenmanagement zugeführt, bleibt die Möglichkeit, Dateien zu signieren.

Das kann ebenfalls mit einem eigenen PGP-Schlüssel erfolgen. Libreoffice integriert das vorbildlich in einer auch für Laien einfachen Art. Doch auch hier gelten die gleichen Herausforderungen beim Schlüsselaustausch wie bei Emails. Ohne diesen können PDF-Betrachter Signaturen zwar sehen, sie jedoch nicht verifizieren.

Hier setzen käuflich zu erwerbende Zertifikate an. Die Wahl des ausstellenden Anbieters entscheidet, ob dieser auf der Adobe Approved Trust List (AATL)[14], der für uns in Europa relevanten eIDAS[15] Trusted-List oder gleich auf beiden geführt ist.

[13] https://media.ccc.de/v/35c3-9463-attacking_end-to-end_email_encryption

[14] https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html

[15] https://eidas.ec.europa.eu/efda/home

Einige wenige proprietären Anwendungen wie der Adobe Acrobat Reader, der Foxit Reader oder ein Microsoft Office können so Dokumente zumindest validieren.

Signierte Dokumente nach eIDAS lassen sich mit dem freien Digital Signature Service (DSS) Framework in Projekte integrieren.[16] Anwendungen können so über eine JSON REST-API Ihre Dokumente signieren und validieren. Im DSS-Cookbook findet sich sogar ein Beispiel für postman.[17]

Nachteil bei allen Lösungen: Eine Integration in bestehende Infrastrukturen und Prozesse ist komplex, die Unterstützung und Akzeptanz insgesamt (noch) zu gering.

Die Konsequenz ist von daher wenig überraschend: Die größte Verbreitung in Unternehmen finden kommerzielle US Online-Dienste wie z.B. Docusign[18], meist beschränkt auf Verträge oder Lizenzen. Eher seltener bei den täglichen “Brot-und-Butter” Belegen wie Rechnungen oder Lieferscheine.

Die freie Alternative dazu wäre LibreSign in Kombination mit dem EU DSS-Framework.[19]

Rechnungs-Portale Kunden- oder B2B-Portale, wo Belege im Webbrowser eingesehen bzw. Heruntergeladen werden können erfreuen sich einer immer größeren Akzeptanz. Unternehmen ermöglichen Ihren Lieferanten oder Kunden Zugriff auf die oftmals selbst betriebenen Lösungen. In kleineren Unternehmen kann das auch eine Nextcloud mit Ordnerfreigabe sein. Die Zugriffe werden verwaltet und 2FA geschützt, was dem aktuellen Stand der Technik entspricht.

Fraglich bleibt, wie bei solchen Portalen der Zustellnachweis bzw. wie Juristen es formulieren, der Zugang erbracht werden kann. Ein Portal, das auf Seiten des Absenders betrieben wird, liegt außerhalb des Einflussbereiches des Empfängers. Das hat Rechtsfolgen was Verzug, Fristwahrung oder Skontoerträge betrifft. Daher sind AGB-Vereinbarungen und daraus abgeleitete Verpflichtungen entscheidend.

[16] https://github.com/esig/dss

[17] https://github.com/esig/dss/blob/master/dss-cookbook/src/main/postman/

[18] https://docusign.com/

[19] https://libresign.coop/

End-to-End Verschlüsselung Last but not least die End-to-End Verschlüsselung, wo nur Absender und Empfänger den Inhalt einer Email lesen können. Das ist die vom OLG in den Raum gestellte Maßnahme. Gewöhnliche Transportverschlüsselungen schützen nach Einschätzung des Gerichts nicht.

Technisch absolut richtig, praktisch aber schwer umsetzbar mit unerwünschten Nebenwirkungen. Der Verlust eines Schlüssel führt unweigerlich zum Totalverlust aller verschlüsselten Emails.

Die beiden technischen Möglichkeiten sind im Abschnitt “Signierte Emails mit S/MIME und PGP” vorgestellt. Ob eine Email signiert oder verschlüsselt ist, entscheidet ein Mausklick.

Fazit

Der aktuelle Fall zeigt, wie das Ignorieren von gängigen und lange bewährten Internet-Standards leichtfertig Haftungs- und Reputationsfallen öffnet. Die erste RFC Spezifikation von S/MIME entstand immerhin vor 27 Jahren im Jahr 1998.[20] Die RFCs von PGP ebenfalls.[21]

Betroffen sind prinzipiell alle, die PDF Rechnungen per Email mit hohen Rechnungssummen verschicken.

Entgegen der Auffassung des OLGs und der Panikmache so mancher Zeitgenossen tendiere ich dazu, Belege wie Rechnungen oder Lieferscheine in einer Email nur zu signieren. Ein defensives, risikobasiertes und minimal-invasives Vorgehen, das für jeden unproblematisch in der Umsetzung sein sollte. Fehler im Umgang mit Schlüsseln belassen die Inhalte zumindest noch zugänglich.

Eine End-to-End Verschlüsselung ist hingegen nur für besonders schutzwürdige oder vertrauliche Daten wie z.B. Passwörter vorbehalten. Prinzipell haben sensible Daten überhaupt nichts in Emails zu suchen, aber das ist eine andere Geschichte.

Signierte Emails geben einem Empfänger die Chance zur Validierung und stellen ein sanftes “KANN”, kein hartes “MUSS” dar. Ohne Zwang zur Nutzung einer bestimmter Software oder Online-Services.

Das Ganze flankiert mit organisatorischen Maßnahmen zum Schutz der eigenen Mitarbeiter und klaren AGB-Regelungen zur Klärung von Haftungsfragen. Gerne auch mit einem Service-

[20] https://datatracker.ietf.org/doc/html/rfc2311

[21] https://datatracker.ietf.org/doc/html/rfc2440

hinweis auf der Website verbunden, wie S/MIME oder PGP signierte Emails mit Fingerprint zu überprüfen sind.

Wer die vom Absender einer Mail angebotene Möglichkeit zur Validierung ignoriert, der muß auch für den Schaden aufkommen. Zur Erinnerung: IT-Sicherheit ist vertragliche Nebenpflicht.[22]

In diesem Sinne,
Tomas Jakobs

[22] https://beck-online.beck.de/Bcid/Y-300-Z-MMR-B-2023-S-761-N-1