Update

November 2014

IT-Recht

VON BOETTICHER
RECHTSANWÄLTE

ZUSAMMENFASSUNG

1. **Haftungsfalle Spam-Ordner**
   - Spam sollte abgewiesen, nicht in Junk-Ordner verschoben werden.
2. **Unzulässige unsichere Verschlüsselung weit verbreitet**
   - Aufsichtsbehörden prüfen auf Verschlüsselung nach dem Stand der Technik.
3. **Deutschsprachige AGB für deutschsprachige Angebote**
   - Deutschsprachige Angebote müssen AGB und Pflichtinformationen auf Deutsch bereitstellen.
4. **Internet-Provider dürfen Überwachungs-Statistiken veröffentlichen**
   - von BOETTICHER belegt: Statistische Angaben zur Internet-Überwachung sind zulässig.

1. Haftungsfalle Spam-Ordner

Unternehmer müssen den Junk-Ordner ihres E-Mail-Postfachs mindestens täglich sichten, ob eine Nachricht versehentlich als Spam markiert worden ist. Das hat das Landgericht Bonn entschieden. Rechtsanwalt Matthias Bergt, IT-Rechtler der Sozietät von BOETTICHER, empfiehlt in der Fachzeitschrift „Der IT-Rechts-Berater“ (ITRB), als Spam erkannte E-Mails gar nicht erst anzunehmen, sondern von vornherein abzuweisen.

Spam-Ordner schaffen für den Nutzer ein großes Problem: Der Empfänger muss sich mit ihrem Inhalt beschäftigen – und zwar mit der gleichen Sorgfalt, mit der er alle anderen Eingänge prüft, was er mit der Einrichtung des Spam-Filters gerade vermeiden wollte. In der Praxis beachten die meisten Empfänger deshalb die Mails im Spam-Ordner überhaupt nicht. Dabei ist eine E-Mail auch dann im rechtlichen Sinne zugegangen, wenn sie nach Annahme mit dem Quittungscode ‚250 – OK’ durch den Empfangs-Server verschoben oder gar gelöscht wird. Sie entfaltet damit alle Rechtswirkungen, auch wenn der Empfänger sie niemals zur Kenntnis nimmt – oder verspätet, wie der Beklagte in einem Verfahren vor dem Landgericht Bonn, der zu knapp 100.000 Euro Schadensersatz verurteilt wurde.

Da kein Unternehmen auf einen Spam- oder einen rechtlich gleich zu behandelnden Viren-Filter verzichten kann, sollten als Spam oder Virus erkannte E-Mails gar

nicht erst angenommen, sondern mittels „Reject“ von vornherein abgewiesen werden: Denn wenn eine Nachricht abgewiesen und gar nicht erst angenommen wird, gelangt sie nicht in den Machtbereich des Empfängers und geht damit rechtlich nicht zu. Der Absender wird informiert, dass seine Mail nicht angekommen ist. Er kann dann sofort reagieren – und erfährt nicht erst beispielsweise bei einer Nachfrage ein paar Tage später, dass seine Mail als Spam behandelt und nicht zugestellt wurde. Auch eine Zugangsvereitelung liegt nicht vor, wenn ein eigentlich ordnungsgemäßer Spam-Filter einzelne Mails fälschlich als Spam behandelt, wie Bergt im ITRB begründet. Der Empfänger kann also auch nicht so behandelt werden, als wenn die versehentlich rejectete Nachricht ihn erreicht hätte.

Wer befürchtet, durch so genannte „false positives“, also als Spam erkannte erwünschte E-Mails, seine Kommunikationspartner zu vergrätzen, kann immer noch einen Mittelweg wählen: Ein nur wenig scharf eingestellter Spam-Filter blockt bereits den allergrößten Teil der unerwünschten Werbe-Mails ab, ohne dass ein ernsthaftes Risiko für false positives besteht. Die verbleibenden Spam-Mails lassen sich problemlos per Hand löschen.

Weiterführende Informationen:

LG Bonn, Urteil vom 10.1.2014, Az. 15 O 189/13

https://www.boetticher.de/14110a

Matthias Bergt: Pflicht zur Prüfung des Spam-Ordners, Der IT-Rechts-Berater (ITRB) 2014, S. 133

https://www.boetticher.de/14110b

2. Unzulässige unsichere Verschlüsselung weit verbreitet

Unternehmen müssen auf ihren Servern Transportverschlüsselung verwenden, etwa HTTPS und STARTTLS – und zwar Verschlüsselung „nach dem Stand der Technik“. Doch bei einem Test des Online-Bankings der 100 größten Banken in Deutschland fielen 78 Prozent in Sachen Sicherheit glatt durch – sie verwendeten unsichere Verschlüsselungsverfahren, die teilweise seit Jahren nicht mehr für vertrauliche Kommunikation eingesetzt werden dürfen.

Der nach dem Gesetz (z.B. in der Anlage zu § 9 BDSG und diversen weiteren Normen) vorgeschriebene Stand der Technik bedeutet unter anderem den Einsatz von Algorithmen, die verhindern, dass abgehörte Kommunikation nachträglich entschlüsselt werden kann, wenn der private Schlüssel abhanden kommt. Dieses Risiko ist keineswegs hypothetisch, wie in den letzten Monaten die beiden katastrophalen Sicherheitslücken Heartbleed und Shellshock zeigten. „Perfect Forward Secrecy“ (PFS) verhindert solche Angriffe.

76 der 100 größten Banken bieten Online-Banking an. Doch nur neun (11,8 Prozent) nutzten zeitgemäße Verschlüsselung, die auch bei Nutzung des Internet Explorers (in seiner aktuellen Version) eine sichere Verschlüsselung mit Perfect Forward Secrecy bietet (ECDHE mit AES). 25 weitere Banken (32,9 Prozent) boten zumindest für Nutzer anderer moderner Browser PFS (DHE mit AES), eine davon allerdings mit einem abgelaufenen Sicherheitszertifikat (zwischenzeitlich behoben). 40 Banken (52,6 Prozent) verwendeten als Verschlüsselungsverfahren dagegen das veraltete RSA mit AES.

Zwei Banken nutzten gar mit RC4 ein Verfahren, das wohl in Echtzeit geknackt werden kann – und das insgesamt 78,4 Prozent der Banken unterstützen, obwohl es bereits seit Jahren nicht mehr für vertrauliche Kommunikation eingesetzt werden darf. Das Problem: Selbst wenn ein WWW-Server standardmäßig eine gute Verschlüsselung benutzt, kann er mittels Downgrade-Angriffen dazu gebracht werden, unsichere Verschlüsselung zu benutzen – allerdings nur, wenn er diese unsichere Verschlüsselung auch unterstützt.

Neben der Verschlüsselungs-Chiffre ist auch das verwendete Protokoll ein Problem: Das unsichere SSL3 ist noch sehr weit verbreitet, teilweise gar – auch im Online-Banking – das gefährliche SSL2. Dass das Verbot, SSL3 für personenbezogene Daten einzusetzen, berechtigt ist, belegte der kürzlich von Google publizierte „Poodle“-Angriff.

Aus den Datenschutz-Aufsichtsbehörden haben wir erfahren, dass diese derzeit automatische Prüfungen vorbereiten, ob HTTPS a) überhaupt und b) korrekt konfiguriert verwendet wird. Bei E-Mail-Servern hat Bayern bereits einige Tausend Unternehmen getestet – und etwa jedem fünften einen „blauen Brief" geschrieben. Die Software dafür gibt Bayern an die Aufsichtsbehörden der anderen Bundesländer weiter.

Weiterführende Informationen:

Vortrag „Verschlüsselung nach dem Stand der Technik als rechtliche Verpflichtung" von Matthias Bergt

https://www.boetticher.de/14110c

Matthias Bergt: Verschlüsselung nach dem Stand der Technik als rechtliche Verpflichtung, CR 2014, S. 726

Matthias Bergt: Konfiguriert eure Server endlich sicher!, CR-Online.de-Blog vom 15.10.2014

https://www.boetticher.de/14110d

Bodo Möller, Thai Duong, Krzysztof Kotowicz: This POODLE Bites: Exploiting The SSL 3.0 Fallback

https://www.boetticher.de/14110e

3. Deutschsprachige AGB für deutschsprachige Angebote

Wer sich mit einem deutschsprachigen Angebot an deutsche Verbraucher wendet, muss auch seine AGB auf Deutsch bereitstellen. Dies hat das Landgericht Berlin in einem Verfahren gegen WhatsApp entschieden. Die Entscheidung lässt sich analog auch auf verbraucherrechtliche Pflichtinformationen anwenden.

Die Verbraucher hätten bei englischsprachigen AGB keine zumutbare Möglichkeit der Kenntnisnahme, so dass die AGB bereits nach § 305 Abs. 2 BGB nicht in den Vertrag einbezogen werden. Ausnahmen dürften nur in Spezialfällen denkbar sein, wenn zu erwarten ist, dass alle Kunden englische Rechtssprache verstehen – allerdings wird in diesen Fällen dann das eigentliche Angebot kaum auf Deutsch sein.

Unternehmen sollten daher, wenn sie ein deutschsprachiges Angebot starten, dieses vollständig auf Deutsch gestalten – einschließlich der AGB und aller verbraucherrechtlichen Pflichtinformationen. Ebenso müssen die deutschen Rechtsvorschriften auch materiell eingehalten werden, was insbesondere bei AGB typischerweise weitgehend vom englischsprachigen Original abweichende Regelungen erfordert. Dazu gehört ebenfalls ein vollständiges Impressum – auch hier wurde WhatsApp verurteilt, weil die Vertretungsberechtigten, die geografische Anschrift, die Telefonnummer und die Angaben zum Registereintrag fehlten. Ausnahmen gelten nur in besonderen Fällen, etwa wenn ein ägyptischer Reiseveranstalter Kreuzfahrt-Ausflüge in Ägypten anbietet, weil hierfür nach Art. 6 Abs. 4 lit. a) Rom-I-VO kein deutsches Recht gilt (so ein Fall, den das LG Siegen entschieden hat).

Weiterführende Informationen:

LG Berlin, Urteil vom 9.5.2014, Az. 15 O 44/13

https://www.boetticher.de/14110f

LG Siegen, Urteil vom 9.7.2013, Az. 2 O 36/13

https://www.boetticher.de/14110g

4. Internet-Provider dürfen Überwachungs-Statistiken veröffentlichen

Auch deutsche Internet-Provider dürfen Statistiken veröffentlichen, in welchem Umfang staatliche Behörden Überwachungsmaßnahmen angeordnet haben. Der E-Mail-Provider Posteo veröffentlichte nun als erster deutscher Internet-Provider einen Transparenzbericht. Noch am selben Tag zogen weitere Anbieter nach. Zuvor hatten nur US-Unternehmen wie Yahoo und Google Transparenzberichte veröffentlicht, weil die herrschende Meinung solche Veröffentlichungen in Deutschland für strafbar hielt.

Nach den Enthüllungen des Ex-NSA-Mitarbeiters Edward Snowden hatten sich verschiedene US-Anbieter bereits das Recht erkämpft, zumindest über nicht ausdrücklich als geheim bezeichnete Überwachungsmaßnahmen in groben Abstufungen zu berichten. Für deut-

sche Anbieter ergaben sich potentielle Hindernisse insbesondere aus Geheimhaltungspflichten gemäß G10-Gesetz, TKG, BVerfSchG, ZfdG und TKÜV.

Ein von-BOETTICHER-Gutachten hat jedoch herausgearbeitet, dass trotz des strengen Gesetzeswortlauts rein statistische Angaben keiner Geheimhaltungspflicht unterliegen. Zweck der Regelungen sei es nur, eine Behinderung konkreter Ermittlungen zu vermeiden. Soweit bestimmte Normen im Sinne umfassender Verschwiegenheitspflichten interpretiert würden, ist dies auf eine Verselbstständigung zurückzuführen, die weder mit dem Wortlaut des Gesetzes noch mit der Intention des Gesetzgebers in Einklang zu bringen ist. Auf eine kleine Anfrage des Bundestagsabgeordneten Hans-Christian Ströbele bestätigte die Bundesregierung die Zulässigkeit der Veröffentlichung statistischer Angaben.

Noch am Tag der Veröffentlichung des Posteo-Transparenzberichts zogen weitere deutsche Provider nach und gaben Zahlen zu staatlichen Überwachungsmaßnahmen bekannt. Zu ihnen gehört die Telekom – sie hatte es noch Anfang Februar abgelehnt, Zahlen zu Überwachungsmaßnahmen zu veröffentlichen.

Weiterführende Informationen:

von-BOETTICHER-Gutachten zur Zulässigkeit von Transparenzberichten

https://www.boetticher.de/14110h

Matthias Bergt: Transparenzberichte zu Internet-Überwachungsmaßnahmen, Computer und Recht (CR) 2014, S. 510

Ansprechpartner:

Wenn Sie Fragen haben oder weitere Informationen zu einem der Themen wünschen, wenden Sie sich bitte an:

Matthias Bergt
E-Mail: mbergt@boetticher.com
Tel. +49 / 30 / 61 68 94 03

Dr. Anselm Brandi-Dohrn, maître en droit
E-Mail: abrandi-dohrn@boetticher.com
Tel. +49 / 30 / 61 68 94 03

oder Ihren üblichen Ansprechpartner bei VON BOETTICHER.

VON BOETTICHER Rechtsanwälte
Oranienstraße 164
10969 Berlin

VON BOETTICHER Rechtsanwälte
Freiherr-vom-Stein-Straße 11
60323 Frankfurt am Main

VON BOETTICHER Rechtsanwälte
Widenmayerstraße 6
80538 München