Verschlüsselte Bestätigungsmails bei Onlinegeschäften

Inhaltsverzeichnis

Dr. Rainer Hammerschmidt, Vorstandsmitglied
MA Beate Baum, Wissenschaftliche Fachberatung

Einleitung: Yes we can - Datenschutz

Nach den Enthüllungen über die Abhör- und Speicherpraxis der Geheimdienste durch Edward Snowden ist die Anzahl der Menschen merklich gestiegen, die sich Gedanken über den Schutz ihrer Daten machen. Viele versuchen auf Cryptoparties Hilfe zu finden, wie sie ihre Daten verschlüsseln können. Aber auch die Anbieter im Internet reagieren.

Die Telekom propagiert das „Deutsche Internet“, ausgerechnet zusammen mit Web.de und 1&1, beides Unternehmen der Firma United Internet. Die Bundesregierung steht weiter zu DE-Mail, der angeblich sicher verschlüsselten E-Mail für Deutschland, wo die Datenpakete bei jedem Provider einmal aus- und dann wieder eingepackt werden - also gerade dort, wo die Abhöreinrichtungen von BKA und Geheimdiensten installiert sind.

Selbst der Datenkrake Google will künftig bei seinem Google-Mail Dienst eine Ende-Zu-Ende Verschlüsselung mit PGP anbieten – hoffentlich kümmert man sich dann bei Google auch um die internen Sicherheitslücken. In Deutschland wurde im Juni 2015 gabel.de vorgestellt, eine Software, die einmal die Vorteile der Sender-/Empfängerverschleierung und Komplettverschlüsselung von Systemen wie Bitmessage, Retroshare, Darknet, i2p usw. mit serverbasierter Datenhaltung verknüpfen und zugleich bedienbar machen soll.

Auch wir haben uns Gedanken gemacht, wie wir neben dem Angebot von Cryptoparties den Datenschutz voranbringen können.

Aktion Freiheit statt Angst hat einen Vorschlag für verschlüsselte Bestätigungsmails bei Onlinegeschäften als IT-Lösung beim Wettbewerb Innovationspreis-IT eingereicht, den die Initiative Mittelstand zur Cebit 2015 ausgeschrieben hatte. Auch 2018 waren wir wieder dabei.

Die Idee hat scheinbar überzeugt, so dass sich unser Vorschlag einige Tage unter den Besten im Bereich IT-Security befand. Ein Grund dafür mag auch sein, dass für unsere Quick&Dirty Realisierung eigentlich nur zwei Zeilen Code notwendig waren - so einfach lässt sich eine sichere Kommunikation herstellen!

Wir hoffen nun auf viele Nutzer dieser Lösung, die unsere Kommunikation sicherer machen kann.

Problem Bestellvorgänge im Internet

Wem als Internetnutzer der Schutz der eigenen Daten wichtig ist, der kann zwar seine E-Mails mit PGP verschlüsseln und Webseiten mit dem Firefox-Plugin HTTPS-Everywhere bevorzugt verschlüsselt oder gar im TOR-Browser abrufen, der Schutz der persönlichen Daten findet jedoch spätestens dann ein Ende, wenn man als Internetnutzer eine Ware in einem Online-Shop bestellt hat. Dann erhält man als Kunde eine (oder mehrere) unverschlüsselte E-Mails, die neben der E-Mail-Adresse, Rechnungs- bzw. Lieferadresse, ggf. Kunden-

nummer und weitere Daten enthalten, insbesondere Informationen zur bestellten Ware.

Diese E-Mail wird nicht zwingend auf direktem Weg zum Kunden übertragen, sondern oft auf erheblichen Umwegen über diverse Internetknotenserver, ggf. auch über andere Länder, Satelliten und gerne auch einmal rund um den ganzen Globus. In jedem vermittelnden Internetknoten - insbesondere auch auf dem Server des eigenen E-Mail-Anbieters - können, diese Informationen ohne großen technischen Aufwand ausgelesen und zur Profilbildung genutzt werden. Warum gibt es diese Bestätigungsmails überhaupt?

Für mich als Kunde ist es eine Bestätigung, dass die von mir auf der Webseite des Anbieters eingegebenen Daten von ihm auch so erhalten wurden. Das erhöht mein Vertrauen in den Bestellvorgang - dies ist aber im allgemeinen von einem Bestellformular auch zu erwarten.

Für den Anbieter erfüllt die Bestätigungsmail zwei Aufgaben: Erstens ist er rechtlich verpflichtet ein Onlinegeschäft zu bestätigen, doch dafür würde eine Mail genügen mit dem Satz „Wir bestätigen Ihre Bestellung von heute (Datum) (Uhrzeit) bei uns“.

Eine Übermittlung von persönlichen Daten oder Kontonummern ist rechtlich nicht notwendig. Daraus folgt übrigens auch, dass eine Mail mit personenbezogenen Angaben nach BDSG unzulässig ist (§3a Datensparsamkeit, keine Zweckbindung zum Geschäft).

Nähere Infos gibt es dazu unter:
https://www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/75_3151.htm

Die zweite Aufgabe der Bestätigungsmail für den Anbieter ist der Beginn der Widerrufsfrist, die für jedes Onlinegeschäft mit der Bestätigung durch den Verkäufer beginnt. Um sich dabei auf der „sicheren Seite“ zu bewegen, schreibt er in diese Widerrufsbelehrung alle für ihn wichtigen Daten des Bestellvorgangs hinein. Zur näheren Erläuterung hier die Stellungnahme einer Juristin beim Projekt www.surfer-haben-rechte.de des Verbraucherzentrale Bundesverband e.V.:

> "Werden personenbezogene Daten im Rahmen von Eingangsbestätigungen eines Online-Shops per E-Mail versendet, müssen nach §9 S. 1 BDSG technische und organisatorische Maßnahmen zur Datensicherheit getroffen werden. Nach Satz 2 Nr. 4 Anlage BDSG muss unter anderem sichergestellt werden, „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“.

Als geeignete Maßnahme nennt Satz 3 Anlage BDSG „insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren“. Nach §9 S. 2 BDSG sind Sicherungsmaßnahmen allerdings nur dann erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzbedürftigkeit der Daten steht. Je höher die Schutzbedürftigkeit, desto höher auch der Aufwand, der noch angemessen ist.

Die Eingangsbestätigung enthält typischerweise mindestens die vollständige Lieferanschrift, bei Verbrauchern meist die Wohnanschrift. Die Anschrift ist ein Datum, das schutzbedürftig ist. In der für einen Online-Shop gebotenen abstrakten Betrachtung kann nicht darauf abgestellt werden, dass kein Schutzbedürfnis besteht, wenn der Kunde seine Anschrift bereits selbst veröffentlicht hat. Es sind stattdessen Vorkehrungen beispielsweise für den Fall zu treffen, dass der Kunde Politiker, Richter oder Stalking-Opfer ist, so dass ein Bekanntwerden seiner Anschrift möglicherweise erhebliche Folgen haben könnte. Auch hat jeder Einzelne das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Darüber hinaus können selbst Daten, die auf den ersten Blick nicht schutzbedürftig erscheinen, unter bestimmten Umständen ein erhebliches Schadenspotenzial haben. Gegen diese Gefährdungslage ist der Aufwand für Sicherungsmaßnahmen abzuwägen. In Betracht käme zum Beispiel der Verzicht auf die Nennung von Daten wie Name, Anschrift oder Bankverbindung in der E-Mail-Bestellbestätigung, da nur die Tatsache des Eingangs einer Bestellung bestätigt werden muss, nicht aber ihr Inhalt einschließlich der Daten des Bestellers.

Eine andere Möglichkeit zur Sicherung wäre eine Verschlüsselung der Bestätigungs-E-Mail. Der Aufwand für die Verschlüsselung ist gering, der Vorteil für den Schutz der Kunden dagegen erheblich, so dass keine Unverhältnismäßigkeit i. S. von §9 S. 2 BDSG vorliegt."

Die Kampagne "For your eyes only"

Im Rahmen dieses Projekts werden Betreiber von Online-Shops aufgerufen, die Privatheit ihrer Kunden technisch besser zu unterstützen, indem sie die Übermittlung PGP-verschlüsselter E-Mails an ihre Kunden anbieten, werden bestehende Cryptoparty-Angebote bekannt gemacht, die in die Verwendung von PGP-Verschlüsselung in Mailprogrammen einführen, werden Wege vorgeschlagen, wie Kunden ihren öffentlichen Schlüssel an die Anbieter der Online-Shops übermitteln (über Keyserver, durch Hochladen beim Bestellvorgang, als Anhang einer E-Mail), wird die Öffentlichkeit über diverse Medienkanäle informiert und dabei die Bedeutung von Verschlüsselung und Datenschutz konkret thematisiert (Pressemeldungen zum Stand der Dinge können in sinnvollen Abständen wiederholt werden und evtl. die Namen derjenigen Shops erwähnen, die bereits eine Mail-Verschlüsselung anbieten), werden Unterstützer für die Kampagne gesucht, die durch Spenden, Öffentlichkeitsarbeit bzw. technische Beiträgen helfen, z.B. die Datenschutzbeauftragen der Länder/des Bundes , Organisatorinnen von Cryptopartys, Campact, Digitalcourage, CCC, SuMa e.V., VZBV/Projekt surfer-haben-rechte, . . .

AKTION Freiheit statt Angst

Aktion Freiheit statt Angst e.V.
Bündnis für Freiheitsrechte, gegen Massen-Überwachung und Sicherheitswahn

Mitglied des
European Civil Liberties Network

Aktion Freiheit statt Angst e.V. wendet sich gegen die zunehmende Überwachung der Menschen durch staatliche und private Stellen.

FOR YOUR EYES ONLY
Verschlüsselte Mails bei Online-Bestellungen

Ein wichtiger Beitrag einer solchen Kampagne besteht auch darin, die Benutzerfreundlichkeit der Verschlüsselungstechnik für den Normaluser zu prüfen und zu verbessern (Veranstalter von Cryptopartys, Enigmail-Forum, ...). Nach den ersten Implentierungen soll auch ein Leitfaden für Admins von Online-Shop-Portalen zur Umsetzung und ggf. Support organisiert werden.

Zur Verbreitung der Kampagne haben wir die zentralen Punkte in einem Flyer beschrieben, der hier zum Download bereit steht.
https://www.aktion-freiheitstattangst.org/images/docs/201409fsaFlyerMailVerschl.pdf

In einem weiteren Schritt sollen die beteiligten Online-Shops belohnt werden, indem sie ihren Shop mit einem Siegel zieren dürfen und ggf. auf einer Liste auf der Kampagnen-Webseite lobend erwähnt werden. Hier sind zur Verwendung eines solchen Siegels noch rechtliche Fragen zu klären, damit niemand sich damit ziert, der nicht die Bedingungen dafür erfüllt.

Ausblick

Mit einer kleinen Verbesserung wird das Internet nicht auf ein Mal zu einem sicheren Ort. Aber es ist ein Anfang und der Erfolg hängt davon ab, ob genügend Online-Shops so eine Lösung oder etwas ähnlich sicheres anbieten. Irgendwann hat jeder Mensch sich ein Schlüsselpaar erzeugt und die Skepsis gegen „Verschlüsselung“ schwindet, es ist dann einfach ein Standard, den man nutzt. Damit wäre schon viel gewonnen.

Um ausreichend Online-Shops zum Mitmachen zu bewegen, muss weiter untersucht werden, ob die derzeitige Praxis überhaupt rechtskonform ist. Wenn, wie wir das vermuten, das nicht der Fall ist, so steht jedermann der Rechtsweg offen, um die Anbieter zu einem rechtlich abgesicherten Be-

stellvorgang zu bewegen.

Die Meinung der Datenschutzbeauftragten wäre in diesem Zusammenhang nicht unwichtig (siehe das übernächste Kapitel „*Antworten auf unsere Anfragen*“).

Unser technischer Lösungsvorschlag

Wie lässt sich nun für einen Onlineshop möglichst einfach und kostengünstig eine verschlüsselte Antwort auf eine Anfrage oder Bestellung erzeugen. Dazu sollen im folgenden drei mögliche Szenarien beschrieben werden, die es erlauben dem Kunden eine verschlüsselte Bestätigungsmail zuzustellen.

Wir unterscheiden „in erster Näherung“ für die Praxiserprobung drei Szenarien, eventuell gibt es weitere Anforderungen, auf die man uns gern hinweisen mag.

- Fall 1: Der Kunde hat seinen Public Key auf einem öffentlichen Keyserver
- Fall 2: Der Kunde möchte seinen Public Key eingeben.
- Fall 3: Der Kunde möchte künftig per Bitmessage kommunizieren.

Für die im folgenden beschriebenen Fälle 1+2 muss der Anbieter PGP oder GnuPG auf seinem Server installiert haben und im Bestellformular neben der Angabe der E-Mail-Adresse des Kunden

- für Fall 1 ein Feld (max. Feldlänge 50, d.h. 40 Zeichen und evtl. 9 Leerzeichen) für den Fingerprint des Public Keys und
- für Fall 2 ein Feld (Textfeld mindestens 30 Zeilen und 65 Zeichen/Zeile) für den Public Key und ein Feld (Textfeld Länge 10) für die Key ID anbieten.

Für den Fall 3 installiert der Anbieter das Programm Bitmessage auf dem Server und bietet im Bestellformular neben der Angabe der E-Mail-Adresse ein Eingabefeld für die Bitmessage Adresse an. Alternativ bei nur einem Eingabefeld für eine „Mail-Adresse“ kann die Software auf dem Server auch prüfen ob es sich um eine E-Mail-Adresse (mit einem @) oder eine Bitmessage Adresse (mit einem BM-) handelt.

Fall 1: Der Kunde hat seinen PGP Public Key auf einem Keyserver

Auf dem Bestellformular gibt der Kunde neben seiner E-Mail-Adresse in das Feld für den Fingerprint des Public Keys seinen Fingerprint ein. Diesen kopiert er sich

- über die Zwischenablage entweder aus seiner Mail-Signatur oder
- bei Verwendung von Enigmail und Thunderbird aus der Schlüsselverwaltung oder
- aus der Kommandozeile mit dem Befehl *gpg --fingerprint eigene@Mailadresse*

Die Software auf dem Server wird dann den Public Key zu dem angegebenen Fingerprint aus dem Internet herunterladen und in den server-eigenen Keyring importieren (z.B. mit dem Befehl gpg --import Pubkey.asc).

Fall 2: Der Kunde möchte seinen PGP Public Key bei der Bestellung eingeben

Auf dem Bestellformular gibt der Kunde neben seiner E-Mail-Adresse in das Feld für den Public Key seinen 7-bit ASCII kodierten Public Key ein.

Dazu kopiert er diesen in die Zwischenablage entweder

- aus einer Datei MeinPublicKey.asc auf seinem Rechner oder
- bei Verwendung von Enigmail und Thunderbird aus der Schlüsselverwaltung mit dem Befehl „Schlüssel in Zwischenablage kopieren“ oder
- aus der Kommandozeile mit dem Befehl
  gpg --export -a MeineMail@... > MeinPublicKey.asc

Ferner wird die 8-stellige Key ID benötigt, das sind die letzten 8 Stellen des Fingerprints, da es sich bei Tests gezeigt hat, dass nicht immer Name und E-Mail-Adresse des Kunden mit den im Schlüssel verwendeten übereinstimmen (alte E-Mail-Adresse im Schlüssel oder die Namensschreibweise mag verändert eingegeben worden sein).

Die Software auf dem Server wird dann den Public Key in ihren Keyring importieren, z.B. mit dem Befehl *gpg --import PublicKey.asc* .

Fall 1+2 - Weiteres Vorgehen auf dem Server

Auf dem Server wird nun der in der Vergangeheit stets unverschüsselt verschickte Textinhalt der Mail mit dem öffentlichen Schlüssel des Kunden verschlüsselt. z.B. mit dem Befehl

cat Mailtext | /usr/bin/gpg -a -o crypt.txt.gpg -e -r KeyID-des-Kunden

Dann kann die Mail an den Kunden verschickt werden, z.B. mit dem Befehl

cat crypt.txt.gpg | mailx -s „Ein nettes Betreff“ Mailadresse@Kunde

Der Anbieter kann, bzw muss aus rechtlichen Gründen, die Mail selbst archivieren. Dies tut er bisher unverschlüsselt, er hat nun die Möglichkeit auch sein Mailarchiv verschlüsselt zu führen. Dazu muss er seinen öffentlichen Schlüssel bei der Verschlüsselung zusätzlich einfügen, z. B. mit dem Befehl

cat Mailtext | /usr/bin/gpg -a -o crypt.txt.gpg -e -r KeyIDdesKunden KeyIDdesAnbieter

Fall 3: Der Kunde möchte über Bitmessage kommunizieren

Dafür hat der Anbieter Bitmessage auf dem Server installiert. Auf dem Bestellformular muss der Kunde die Wahl für die Eingabe einer E-Mail oder einer Bitmessage Adresse haben. Gibt er eine Bitmessage Adresse ein, so wird die Bestätigungsmail per Bitmessage an diese Adresse verschickt.

Da Bitmessage nur verschlüsselte Nachrichten kennt, ist damit das Problem erledigt. Eine Eingabe von Passwörtern oder Schlüsseln ist hier nicht erforderlich.

Offen sind in diesem Fall jedoch evtl. rechtliche Fragen, z.B. ob

- eine Bitmessage von Gerichten wie eine E-Mail als rechtsverbindlich angesehen wird,
- die lokale Kopie einer Bitmessage für die Widerrufsbelehrung als rechtlich abgesichert gilt. Was gilt bei Bitmessages als Versanddatum und Zeitpunkt der Zustellung?

Realisierung als Beispiel auf unseren Webseiten

Wir sind dabei die oben beschriebenen Wege auf unserer Webseite zu implementieren. Wir verkaufen zwar nichts, aber wer unsere Arbeit als unterstützenswert ansieht, kann uns Online eine Spende zukommen lassen, die wir per Lastschrift von ihrem/seinen Konto einziehen.

Diese Webseite haben wir als Test für die oben beschriebenen Wege verwendet und ebenso unseren Online-Mitgliedsantrag auf dem auch persönliche Daten abgefragt werden und die Bestellseite für DVDs unseres FRONTex-Films mit der Möglichkeit zur Eingabe eines öffentlichen Schlüssels (PublicKey) versehen.

Wir freuen uns jetzt natürlich über viele Tester und auch über echte Spenden, nehmen aber in den

nächsten Monaten auch gern Spenden über 0,00€ an, um allen die Möglichkeit zum Ausprobieren von solchen sicher verschlüsselten Bestätigungsmails zu geben.

Offene Fragen/Verbesserungsvorschläge

Im Verlauf der Überlegungen zu diesem Thema und bei den konkreten Implementierungen sind zum einen eine Reihe von Fragen entstanden und zum anderen Ideen zu Verbesserungen bei den derzeitigen Implementierungen der E-Mail-Verschlüsselung, z.B. in der Kombination des Programms Enigmail mit Thunderbird.

Diese wollen wir hier ohne Wertung, aus Zeitmangel sowie unvollständigem Know-How über die jeweiligen Implementierungen ohne eine tiefer gehende Untersuchung auflisten:

Fragen zu PGP/GnuPG

- Wie viele Schlüssel können in einen Keyring importiert werden?
- Was passiert bei "Uneinigkeit" über die Gültigkeit eines Schlüssels?
- Es ist möglich, Schlüssel von Schlüssel-Servern herunterzuladen, die bereits widerrufen wurden, ohne dass man einen Warnhinweis erhält.
- Hier stellt sich zum einen die Frage, warum widerrufene Schlüssel noch auf den Schlüsselservern liegen und nicht automatisch gelöscht werden.
- Antwort: Schlüssel müssen "ewig" auf den Keyservern bleiben. Es kann ja immer mal sein, dass eine alte Signatur geprüft werden muss oder man wissen muss, für wen etwas verschlüsselt wurde.

Fragen zur Funktionalität von Enigmail mit Thunderbird

Enigmail sollte intuitiv bedienbar werden, das ist nach den gemachten Erfahrungen derzeitig nicht ganz der Fall. Einige Hinweise und Fragen:

- Unterschreiben von Schlüsseln: Hat ein User mehre PrivateKeys und möchte den PublicKey eines anderen unterschreiben so kann der User nicht auswählen mit welchen seiner Keys er unterschreiben kann.
- Bei Bedienfehler werden versehentlich Mails unverschlüsselt versendet. Eine Bestätigung vor dem Senden sollte immer angezeigt werden.
- Probleme bei extern verschlüsselten Anhängen in verschlüsselten Mails, manchmal bis zum Absturz von Thunderbird.
- Die Ursache könnte in Kombinationen von Utf-8 und Winxx59 Bodyparts liegen?
- Problem "Besitzervertrauen": Enigmail unter Linux sieht alle nicht explizit vertrauten Schlüssel als ungültig an. Bis inklusive Version 1.6 war es nicht möglich, an ungültige Schlüssel zu verschlüsseln. (mehr Details)
- Wenn man zum Verschlüsseln einer Email einen Schlüssel auswählen möchte (ohne Empfängerregel), kann man unter *OpenPGP / Schlüssel verwalten* die möglichen Schlüssel anzeigen lassen. Dabei werden nur die Schlüssel-ID, Typ, Schlüsselgültigkeit, Besitzervertrauen, Ablaufdatum und Fingerprint angezeigt.
- Die Spalte mit den Namen wird erst angezeigt, wenn das Fenster ausreichend vergößert oder maximiert ist.
- Habe konkret die Erfahrung gemacht, dass ich den Schlüssel nicht auswählen kann, wenn ich das Besitzervertrauen nicht festgelegt habe.
- Wenn man eine Email an einen Empfänger schreiben will, dessen Schlüssel man erst importieren muss, kann man dessen Besitzervertrauen erst danach festlegen.
- Man den Kontext der Email verlassen, damit im Thunderbird Menü der Eintrag *Schlüssel*

verwalten zugänglich ist. Das ist sehr umständlich.
- Beim Exportieren des öffentlichen Schlüssels als Textdatei gibt es keinen expliziten Hinweis darauf, dass wirklich nur der öffentliche Schlüssel exportiert wird.
- ...

Probleme in der Verschlüsselungs-Software

Wir nennen hier Bugs, die in der Presse genannt werden, können aber aus Zeitgründen nicht verfolgen, ob und wenn ja, welche Lösungen dafür in der Zwischenzeit angeboten werden. Wir sind für entsprechende Hinweise dankbar!

- Enigmail, das Thunderbird-Plugin für die Verschlüsselung, hat in der Version 1.7.0 einen Bug. Bitte tauschen gegen die Version 1.7.2.
- Die blind carbon copy (bcc) versendet statt verschlüsselter Mails den Klartext (s. heise.de/newsticker..."Enigmail"). Dies ist inzwischen behoben.
- Bei Poodle/ Pudel ist SSL3 corrupted! Deshalb sollte man besser TLS 1.2. nutzen, wenn im Browser nicht vorhanden, dann TLS 1.0 nehmen. So hat z.Zt. IN-Berlin den Zugriff über SSL 3 "verboten".

Allgemeine Empfehlungen

- Wer verschlüsseln kann und will, sollte das auch in seiner Mail-Signatur angeben.
- Sobald man seine Mails verschlüsseln kann, sollte man seinen PublicKey an alle Kommunikationspartner verschicken. (Am besten mit der Drohung künftig nur noch auf verschlüsselte Mails zu antworten ;-)

Antworten auf unsere Anfragen

Zu Beginn der Kampagne haben wir eine Anfragen an die Datenschutzbeauftragten und die Verbraucherzentrale geschickt. Hier dokumentieren wir die Antworten und wollen diese in der nächsten Zeit bewerten und Folgerungen für die Realisierung der Initiative ziehen.

Der Berliner Beauftragter für Datenschutz und Informationsfreiheit

Der Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4-10, 10787 Berlin

Verschlüsselte Bestätigungsmails im Onlinehandel

Ihr Schreiben vom 26. Oktober 2014

Sehr geehrter Herr Dr. Hammerschmidt,

wir kommen auf Ihr oben genanntes Schreiben zurück, mit dem Sie uns über Ihre Initiative „For your eyes only - Verschlüsselte Bestätigungsmails bei Onlinegeschäften" aufmerksam gemacht haben. Auch wir haben zu diesem Problem schon Eingaben erhalten.

Nach § 312i Abs. 1 Satz 1 Nr. 3 des Bürgerlichen Gesetzbuches (BGB) ist der Zugang einer Bestellung unverzüglich auf elektronischem Wege zu bestätigen. Eine Wiedergabe des Inhalts der Bestellung ist jedenfalls nicht erforderlich, da Sinn der Vorschrift nur ist, dem Kunden Gewissheit darüber zu verschaffen, dass der Unternehmer seine Bestellung erhalten hat (ebenso Bergt, Schutz personenbezogener Daten bei der E-Mail-Bestätigung von Online-Bestellungen, NJW 2011, 3752, 3753).

Die vorstehend genannte Rechtsvorschrift beinhaltet keine weiteren Vorgaben hinsichtlich der Art und Weise der elektronischen Bestätigung, sodass hier ergänzend die datenschutzrechtlichen Vorschriften herangezogen werden müssen. Nach § 9 des Bundesdatenschutzgesetzes (BDSG) sind die erforderlichen technisch-organisatorischen Maßnahmen zu treffen. Einschränkend wird in dieser Rechtsvorschrift allerdings ausgeführt, dass Maßnahmen nur erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Die Datenschutzbehörden haben mit Blick auf den Schutzzweck des Bundesdatenschutzgesetzes ein weites Verständnis zur Erforderlichkeit von technisch-organisatorischen Maßnahmen. Insofern empfehlen wir Unternehmen generell, nicht unverschlüsselt per E-Mail zu kommunizieren und schon gar nicht personenbezogene Daten in solche E-Mails aufzunehmen.

Eine Durchsetzung dieser Empfehlung durch eine behördliche Anordnung konnte bisher jedoch von uns nicht erreicht werden, denn die verwaltungsgerichtliche Entscheidungspraxis hat erkennen lassen, dass bei einer branchenüblichen Art und Weise der Versendung die Einforderung von Verschlüsselung als nicht verhältnismäßig angesehen wird (vgl. VG Berlin, Urteil vom 24.05.2011, Az. 1 K 133.10 zur Ablehnung einer Verschlüsselungspflicht von Bewerberdaten, die von einem privaten Arbeitsvermittler an potentielle Arbeitgeber versandt werden).

Aus diesem Grund würde das Verwaltungsgericht vermutlich auch eine Anordnung im E-Commerce Bereich von uns aufheben, die im Gegensatz zu sensiblen Bewerberdaten „nur einfache Bestelldaten" umfassen würden. Das für uns zuständige Verwaltungsgericht Berlin nimmt eher einen unternehmerfreundlichen Standpunkt ein und stellt hinsichtlich der Erforderlichkeit der technisch-organisatorischen Maßnahmen maßgeblich darauf ab, ob die von der verantwortlichen Stelle geforderte Handlung sich in der Praxis als alltagstauglich erweist.

Damit verbunden ist immer die Frage nach dem finanziellen und organisatorischen Aufwand für die betroffene Stelle sowie ob solche Forderungen praktisch den Geschäftsverkehr zum Erliegen bringen würden. Dies würde sowohl für die Frage der Verschlüsselung als auch für die Begrenzung des Inhalts der Bestätigungs-Mail auf bestimmte Bestelldaten gelten. Vor diesem Hintergrund ist Ihre Initiative für uns sehr interessant.

Verbraucherzentrale Berlin

Verbraucherzentrale Berlin e.V.
Hardenbergplatz 2,10623 Berlin

Ihr Schreiben vom 26.10.2014 Sehr geehrter Herr Dr. Hammerschmidt,
wir bedanken uns für Ihre o. g. Nachricht und teilen Ihnen zunächst mit, dass das Projekt „Surfer haben Rechte" auf eine Initiative des Verbraucherzentrale Bundesverband zurückzuführen ist. Das Projekt wird vom Bundesministerium der Justiz und für Verbraucherschutz finanziell gefördert.

Auch uns ist es ein Anliegen, die Menschen auf die Gefahren für ihre persönlichen Daten bei unverschlüsselter Kommunikation hinzuweisen und weitere Menschen für die Verschlüsselung ihrer Daten zu interessieren. In unseren Publikationen weisen wir regelmäßig darauf hin, dass Datensparsamkeit im Umgang mit den neuen Medien eine Notwendigkeit darstellt.

Schon das Bundesverfassungsgericht stellte in einem Leitsatz fest: „Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" (BVerfG, 1 BvR 370/07 vom 27.02.2008). Dieses Grundrecht steht jedem Bürger zu und ist damit auch eine Verpflichtung für den Staat und nicht nur eine Aufgabe der Bürger allein.

Entsprechende Forderungen nach einem solchen Recht werden bereits seit Jahren von Verbraucher- und Datenschützern gefordert. Die bisherige Praxis der unverschlüsselten Kommunikation im Geschäftsverkehr entspricht jedenfalls nicht den Anforderungen des Datenschutzes.

Rechtlich ist noch Vieles ungeklärt bzw. befindet sich auf dem Weg zur Klärung wie beispielsweise die Frage, ob IP-Adressen personenbezogene Daten sind. Viele Webseiten speichern die IP-Adressen der Besucher. In § 15 Telemediengesetz heißt es dazu, dass personenbezogene Daten nur mit Einwilligung des Nutzers und nur dann gespeichert werden dürfen, wenn sie zur Abrechnung oder ähnliches nötig sind. Die Frage wird gerade durch einen Vorlagebeschluss des BGH, Urteil vom 28.10.2014 - VI ZR 135/13, vom Europäischen Gerichtshof geprüft.

Wir haben allerdings erheblich Zweifel, ob die Benutzerfreundlichkeit vorhandener Verschlüsselungstechniken für den Normalverbraucher bereits so ausgereift ist, dass sich diese Techniken auf breiter Front anwenden lassen. Hier ist noch viel Verbesserungsarbeit notwendig.

Ihre aufgeworfenen Fragen beantworten wir wie folgt: Die Informationspflichten bei Fernabsatzverträgen sind in § 312d BGB i. V. m. den Artikeln 246 a und 246 b des Einführungsgesetzes zum Bürgerlichen Gesetzbuch geregelt.

Bei der Frage der Haftung der Shop-Betreiber für das unverschlüsselte Versenden personenbezogener Daten kommt es darauf an, ob der Betreiber schuldhaft gehandelt hat. Um dies beurteilen zu können, müssten die gesamten Umstände des Einzelfalls beachtet werden. Es müsste insbesondere ein bezifferbarer Schaden adäquat ursächlich entstanden sein.

Fraunhofer-Institut für System- und Innovationsforschung

Koordinator Sicherheitsforschung und Technikfolgenabschätzung
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48 | 76139 Karlsruhe

Sehr geehrter Herr Hammerschmidt,

mit der Anlage zu Ihrer Mail vom 5. November haben Sie einige Fragen an uns adressiert und um Unterstützung bei der juristischen Klärung gebeten.

Nach erfolgter Rücksprache im Projektkonsortium kann ich Ihnen dazu heute antworten. Gleichwohl muss ich vorausschicken, dass Sie im Zweifelsfall anwaltlichen Rat einholen sollten, den wir nicht geben können und der uns letztlich auch nicht zusteht. Zu den Fragen:

1) Welche Daten muss eine Bestätigungsmail rechtlich mindestens enthalten?

Wird zwischen einem Unternehmer und einem Besteller ein Vertrag im elektronischen Geschäftsverkehr abgeschlossen, so bestimmen sich die Informationspflichten des Unternehmers nach der Vorschrift des § 312i Abs. 1 Nr. 3 BGB. Die den Bereich des E-Commerce tangierende nationale Rechtsvorschrift ist Ausfluss der Richtlinie über den elektronischen Geschäftsverkehr 2000/31/EG (E-Commerce-Richtlinie).

Durch § 312i Abs. 1 Nr. 3 BGB wird jeder Unternehmer verpflichtet, dem Kunden den Zugang einer Online-Bestellung ohne schuldhaftes Zögern auf elektronischem Wege zu bestätigen. Der Verbraucher hat folglich einen Anspruch auf Übersendung einer Bestätigung bezüglich der durch ihn vorgenommenen Bestellung. Eine inhaltliche Konkretisierung darüber, auf welchem Wege und welche Angaben inhaltlich gegenüber dem bestellenden Kunden zu treffen sind, wird weder durch die Norm selbst noch durch die Richtlinie festgelegt.

Dem Unternehmer ist jeder elektronische Weg eröffnet. Es genügt daher grundsätzlich auch die Anzeige einer Bestätigungsseite nach Aufnahme der Bestellung auf einer Website.

Nach dem Wortlaut des § 312i Abs. 1 Nr. 3 BGB ist die Angabe von Kundenkontaktdaten, Bestellgegenstand, Bankverbindung u.ä. gegenüber dem Kunden nicht erforderlich, da lediglich der „Zugang“ der Bestellung zu bestätigen ist und gerade nicht deren Inhalt. Normzweck des § 312i Abs. 1 Nr. 3 BGB ist es, den Kunden darüber zu informieren, dass seine Bestellung eingegangen ist, um Unsicherheit und unnötige weitere Bestellungen zu vermeiden. Die Eingangsbestätigung hat keinerlei Dokumentations- oder gar Beweisfunktion, so dass Text- oder gar eine strengere Form nicht erforderlich ist. Die Eingangsbestätigung ist eine reine Wissenserklärung und führt – sofern sie nicht mit einer Annahmeerklärung verbunden wird – nicht zu einem Vertragsschluss. Dementsprechend muss eine Bestätigungsmail keinerlei Mindestinhalt enthalten.

2) Können Shop-Betreiber für das unverschlüsselte Versenden von personenbeziehbaren Daten haftbar gemacht werden?

Ja, durchaus. Entscheidet sich der Unternehmer für die Zusendung einer Bestätigungsmail, so ist zu beachten, dass sämtliche in der Mail enthaltenen Bestelldaten wie z.B. Kontaktdaten des Kunden, vereinbarte Zahlungsmodalitäten und Bankdaten personenbezogene Daten darstellen, auf welche die datenschutzrechtlichen Vorschriften des Bundesdatenschutzgesetzes (BDSG) Anwendung finden.

Die E-Mail-Adresse des Kunden selbst kann hierbei ebenfalls ein personenbezogenes Datum darstellen, sofern sie einer bestimmten Person zugeordnet werden kann. Dies ist insbesondere bei Verwendung einer E-Mail-Adresse mit Klarnamen der betroffenen Person der Fall.

Während das E-Commerce-Recht die Aufnahme von Bestelldaten in eine Eingangsbestätigung nicht verlangt, ist aus datenschutzrechtlicher Perspektive der Versand unverschlüsselter E-Mails, welche personenbezogene Daten enthalten, rechtlich problematisch. Dies ergibt sich aus dem BDSG, das in § 9 BDSG und insbesondere in der Anlage technisch-organisatorische Maßnahmen regelt, um die Einhaltung der gesetzlichen Datenschutzvorschriften sicherzustellen.

Im Falle der Anwendbarkeit des BDSG treffen den Unternehmer gesonderte Pflichten beim Umgang mit den personenbezogenen Daten des Bestellers: Relevant ist im vorliegenden Zusammenhang insbesondere die Notwendigkeit einer Weitergabekontrolle gem. § 9 S. 2 Nr. 4 der Anlage BDSG. Der Betreiber des Onlineshops hat zu gewährleisten, dass die personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine geeignete Maßnahme zur Verhinderung dieser Risiken ist hierbei insbesondere die Verwendung von Verschlüsselungsverfahren, die dem Stand der Technik entsprechen. Der Onlineshop-Betreiber hat Sorge dafür zu tragen, einen Telekommunikationsdiensteanbieter zu wählen, welcher ein angemessenes Schutzniveau beim Versand von E-Mails gewährleistet.

Da eine unverschlüsselte E-Mail von Unbefugten gelesen, kopiert oder verändert werden kann, birgt der Versand personenbezogener Daten in dieser Form Haftungsrisiken.

Werden die datenschutzrechtlichen Vorgaben verletzt, kann der Betroffene deshalb ein gerichtliches Verfahren betreiben. Der Betreiber des Onlineshops kann nicht nur Unterlassungs-, sondern auch Schadensersatzansprüchen ausgesetzt sein.

Schadensersatzansprüche des Betroffenen gegen das Unternehmen können sich zunächst aus der allgemeinen vorvertraglichen und vertraglichen Anspruchsgrundlage des § 280 BGB ergeben. Dem Versender einer unverschlüsselten E-Mail wird es kaum gelingen, den Entlastungsbeweis nach § 280 I S. 2 BGB zu führen. Weitere denkbare Anspruchsgrundlagen können sich aus deliktischer Haftung ergeben, insbesondere aus § 823 I BGB wegen Verletzung des allgemeinen Persönlichkeitsrechts, aber auch aus § 823 II BGB i.V.m. § 9 BDSG. Lediglich in sehr schwerwiegenden Fällen wird im Zusammenhang mit Eingangsbestätigungen auch ein Schmerzensgeldanspruch in Betracht kommen.

Zudem enthält § 7 BDSG einen speziellen deliktischen Anspruch gegen die verantwortliche

Stelle (§ 3 VII BDSG), also das Unternehmen. § 7 S. 2 BDSG enthält eine Beweislastumkehr: Das Unternehmen muss demnach beweisen, dass es die nach den Umständen des Falls gebotene Sorgfalt beachtet hat. Analog § 1004 BGB kann der Betroffene auch Unterlassung der unzureichend gesicherten Verarbeitung seiner Daten verlangen, mit den entsprechenden Kosten für Abmahnung und gegebenenfalls gerichtliche Geltendmachung.

3) Sehen Sie rechtliche oder andere Hindernisse, die unserer Initiative im Wege stehen?

Eine (umfassende) rechtliche Beratung Ihrer Initiative wird durch das Forum Privatheit nicht vorgenommen. Insofern wird eine (fach-)anwaltliche Beratung nahegelegt.

4) Welche Wege bieten sich an, um diese Idee bekannt und populär zu machen?

Die Bekanntmachung Ihrer Initiative in den einschlägigen Datenschutzkreisen sowie die Einspeisung Ihrer Arbeitsergebnisse in selbige bietet eine fruchtbare Möglichkeit, die von Ihnen gewünschte Breitenwirkung zu erreichen.

Auswertung der Antworten

Da sind wir noch dabei - aber klar ist, wir sind auf einem guten Weg und es ist viel möglich. Inzwischen hat sich auch mindestens ein Onlineshop-Betreiber gemeldet, der über eine Implementierung nachdenkt.

Wir sind für Anmerkungen und Kritiken und Verbesserungsvorschläge offen. Bitte einfach per Mail an kontakt@aktion-fsa.de

Ähnliche Lösungen in der weiten Welt

Inzwischen haben die E-Mail-Anbieter gmx.de und web.de eine Ende-zu-Ende Verschlüsselung mit PGP, GnuPG im Angebot. Verwendet werden dazu die Browsererweiterungen Mailvelope und Mailpile.

Auch der vertrauenswürdige E-Mail Anbieter Posteo bietet verschlüsselte E-Mail an. Bei Posteo ist auch der Upload der öffentlichen Schlüssel auf einen Posteo-Server möglich, wenn man den Key-Servern in der weiten Welt misstraut.

Wer lernen möchte, wie Mail-Verschlüsselung funktioniert, kann gern auf unseren Cryptopartys vorbeikommen. Die nächste ist auf jeden Fall zur Engagementwoche im September und dann wieder zum Safer Internet Day im Februar, jeweils ab 19h im Café COOP, Rochstr. 3, 10178 Berlin. Die genauen Termine stehen in unserer Terminliste.

Linksammlung

Der Artikel auf unserer Webseite
https://www.aktion-freiheitstattangst.org/de/articles/4515-20141022-yes-we-can-datenschutz.htm

Unser Flyer „For your eyes only“
https://www.aktion-freiheitstattangst.org/images/docs/201409fsaFlyerMailVerschl.pdf

Innovationspreis der Initiative Mittelstand
http://www.innovationspreis-it.de/

Qabel.de
https://de.wikipedia.org/wiki/Qabel

Surfer haben Rechte
www.surfer-haben-rechte.de

Thunderbird
https://www.thunderbird.net/de/

Enigmail
https://www.enigmail.net/index.php/en/

Mailvelope
https://www.mailvelope.com/

GnuPG
https://www.gnupg.org/

Bitmessage
https://de.wikipedia.org/wiki/Bitmessage
https://bitmessage.ch/