DATENSCHUTZ-NEWS – JANUAR 2017

WICHTIG

Pflichtangabe Online-Streitbeilegung ab dem 01.02.2017

Ein Unternehmer, welcher eine Website unterhält oder Allgemeine Geschäftsbedingungen verwendet, hat den Verbraucher gemäß § 36 Abs. 1 VSBG (Verbraucherstreitbeilegungsgesetz) leicht zugänglich, klar und verständlich in Kenntnis davon zu setzen, inwieweit er bereit oder verpflichtet ist, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Grundsätzlich sind Unternehmer zur Teilnahme an Schlichtungsverfahren nicht verpflichtet. Der deutsche Gesetzgeber hat sich mit dem VSBG dagegen entschieden, Unternehmer grundsätzlich zur Teilnahme an der Alternativen Streitbeilegung zu verpflichten. Ausnahmen gelten jedoch für bestimmte Wirtschaftsbereiche (z. B. für Energieversorger, vgl. dazu § 111b n. F. des Energiewirtschaftsgesetzes – EnWG und für Gasversorger, § 2 Abs. 3 Satz 4 Nr. 4 Gasgrundversorgungsverordnung – GVV).

Wo muss informiert werden?
Der jeweilige Hinweis (siehe nachfolgend A. und B.) muss leicht zugänglich zur Verfügung gestellt werden. Es ist daher zu empfehlen, den Hinweis sowohl in das Impressum als auch in die Allgemeinen Geschäftsbedingungen aufzunehmen.

A: Nicht verpflichtet zur Teilnahme an der Online-Streitbeilegung

Sofern Sie sich nicht vertraglich zur Teilnahme an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle verpflichtet haben, müssen Sie auch nicht an solchen Streitbeilegungsverfahren teilnehmen. Derzeit raten wir aus verschiedenen Gründen auch grundsätzlich davon ab:

- ✓ zu teuer
- ✓ diverse Manipulationsmöglichkeiten (durch Wettbewerber)
- ✓ noch nicht bewährt in der Praxis

Daher empfehlen wir Ihnen, stellen Sie nachfolgenden Text mitsamt anklickbarem Link auf Ihre Website, direkt unterhalb Ihrer Impressumsangaben:

> *Die EU-Kommission stellt eine Plattform zur Online-Streitbeilegung (OS) bereit, die Sie unter http://ec.europa.eu/consumers/odr finden. Die OS-Plattform dient als Anlaufstelle zur außergerichtlichen Beilegung von Streitigkeiten betreffend vertraglicher Verpflichtungen, die aus Online-Kaufverträgen erwachsen.*
>
> *Wir sind zur Teilnahme an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle weder verpflichtet noch bereit.*

B: Ausnahme: Sie haben sich vertraglich zur Teilnahme verpflichtet

Für Sie kommt eine Verpflichtung zur Teilnahme nur dann in Betracht, wenn Sie sich vertraglich zur Teilnahme an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle verpflichtet haben – etwa durch Mediations- bzw. Schlichtungsabreden oder aufgrund des Anschlusses an einen Verband/Verein, in dessen Satzung für alle Mitglieder eine Teilnahme an einer solchen Streitbeilegung vorgeschrieben ist.

Sollten Sie sich also vertraglich verpflichtet haben, stellen Sie nachfolgenden Text mitsamt anklickbarem Link auf Ihre Website, direkt unterhalb Ihrer Impressumsangaben:

> *Die EU-Kommission stellt eine Plattform zur Online-Streitbeilegung (OS) bereit, die Sie unter http://ec.europa.eu/consumers/odr finden. Die OS-Plattform dient als Anlaufstelle zur außergerichtlichen Beilegung von Streitigkeiten betreffend vertraglicher Verpflichtungen, die aus Online-Kaufverträgen erwachsen.*
>
> *Wir nehmen an einem Streitbeilegungsverfahren vor der Verbraucherschlichtungsstelle (hier Angabe von Anschrift und Kontaktdaten der zuständigen Verbraucherschlichtungsstelle) teil.*

Sicherheitslücke im Facebook-Messenger

Eine kürzlich bekanntgewordene Sicherheitslücke im Facebook-Messenger zeigt einmal mehr die Probleme bei der Ende-zu-Ende-Verschlüsselung.

Seit September 2016 bietet der Messenger die Möglichkeit an, Nachrichten Ende-zu-Ende zu verschlüsseln. Jedoch gilt dies nur für neue Chats und alle Beteiligten müssen diese Funktion in den Einstellungen aktiviert haben. Dies gilt jedoch nicht für bestehende Chats.

Weiterhin können verschlüsselte Gespräche nur auf einem Gerät gelesen werden. Die Ende-zu-Ende-Verschlüsselung gilt nicht Geräte-übergreifend.

Mit Hilfe eines sogenannten Cross-Origin-Bypass-Angriffs war es grundsätzlich möglich Inhalte von Facebook Messenger Konversationen über eine externe Webseite mitzulesen. Zwischenzeitlich wurde dieser Fehler durch Facebook behoben.

Quelle: intersoft consulting services AG

Heartbleed immer noch aktuell

Eine Analyse der öffentlich im Internet erreichbaren Systeme zeigt, dass immer noch Hunderttausende für die OpenSSL-Lücke Heartbleed anfällig sind. Die Lücke wird im April bereits drei Jahre alt, jedoch scheint es immer noch Administratoren zu geben, die entsprechende Sicherheitsupdates nicht eingespielt haben.

Die Lücke findet sich derzeit hauptsächlich in Mietservern der Cloud wie bspw. in Amazons AWS-Cloud. Betroffen sind auch Kunden-Server von Verizon oder Strato.

Deutschland belegt derzeit Platz 4 der Heartbleed-Statistik. Insgesamt stammen 14.072 der angreifbaren Server aus Deutschland.

Quelle: www.heise.de

Deutsche Online-Shops angegriffen

Über 1000 deutsche Online-Shops wurden laut BSI-Informationen so manipuliert, dass Kundendaten und Zahlungsinformationen beim Bestellvorgang an Online-Kriminelle weitergeleitet werden.

Betroffen sind die Betreiber, welche Magento (eine Online-Shop-Software) in veralteten und akut angreifbaren Versionen einsetzen. Die Täter haben dadurch die Möglichkeit, beliebigen Code in die Shops einzuschleusen.

Bereits im Oktober 2016 wurden die Shop-Betreiber auf die Gefährdung hingewiesen. Jedoch wurden die betroffenen Kunden nicht über das Problem informiert sowie keine Abhilfe geschaffen. Denn allein die Zahl der in Deutschland betroffenen Online-Shops ist von 500 auf über 1000 gestiegen.

Quelle: www.heise.de

Überwachungsfirma gehackt

Betroffen ist das israelische Unternehmen Cellebrite, welches sich vor allem mit Software für das Auslesen von Daten auf Smartphones einen Namen gemacht hat und zur Überwachungsindustrie zählt.

Die gehackten Daten umfassen Kundeninformationen einschließlich Log-Ins und Passwörter sowie eine Menge technischer Informationen zu Produkten von Cellebrite.

Das Unternehmen hat mittlerweile eingeräumt, dass sich Unbekannte „unautorisierten Zugang zu einem externen Webserver" verschafft hätten.

Quelle: www.heise.de

Abrechnung an falsche Apotheke

Beim Digitalen Rezept Zentrum (DRZ), welches zum Softwarehaus Pharmatechnik gehört, hat eine Mitarbeiterin versehentlich eine Rechnung an die falsche Apotheke versandt. In dieser Rechnung war aufgelistet, wie viele Rezepte von welchen Ärzten ausgestellt werden und welcher Rohertrag sich für die Apotheke ergibt.

Die Apotheke hatte den Vorfall unverzüglich beim Rechenzentrum gemeldet.

Mittlerweile hat sich dieses bei beiden Apotheken entschuldigt.

Quelle: www.apotheke-adhoc.de