UIMCommunic@tion

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Verschlüsselte Internetseiten erhöhen Vertrauen, Sicherheit und Compliance

Ein Unternehmen ohne eigene Internetpräsenz ist kaum noch vorstellbar. Wie eine Visitenkarte und ein eigener Briefkopf, so gehört die eigene Homepage zum Auftritt am Markt. Kunden, potentielle Mitarbeiter, aber auch die unternehmerische Konkurrenz verschaffen sich einen Eindruck über Leistungen und Angebote des Unternehmens im WorldWideWeb. Eine Homepage ist heutzutage schnell gestaltet und noch schneller online gestellt. Datenschutz- und Informationssicherheitsexperte Dr. Jörn Voßbein mahnt jedoch mit dem alten Grundsatz von „Gründlichkeit vor Schnelligkeit" vor unüberlegten Schnellschüssen. „Die Verschlüsselung von Datentransfers gehört in ein Online-Konzept", erinnert Dr. Voßbein an das Telemedien- (TMG) und Bundesdatenschutzgesetz (BDSG).

Bei Aufbau und Betrieb der Firmen-Homepage ist u. a. das Telemediengesetz zu beachten. Was bedeutet das nun für eine Internetpräsenz? Das Telemediengesetz sagt in § 13 Absatz 4 Nr. 3 eindeutig aus, dass „der Nutzer Telemedien gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen kann". Was sind Telemedien? Neben dem reinen Angebot von Informationen auf Unternehmenshomepages sind auch Online-Angebote von Waren und Dienstleistungen mit unmittelbarer Bestellmöglichkeit; Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen; kommerzielle Verbreitung von Informationen über Waren-/Dienstleistungsangebote mit elektronischer Post Dienste im Sinne des Telemediengesetzes.

Mit Absatz 7 wurde die Forderung nach Sicherheitsmaßnahmen für den Nutzer noch einmal verschärft und bekräftigt. Die Maßnahmen müssen zwar angemessen, also technisch möglich und wirtschaftlich zumutbar sein. Der zweite Satz von Absatz 7 macht es dann aber nochmal sehr deutlich, was der Gesetzgeber von einem Telemedien-Betreiber erwartet: „Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens." Diese Formulierung hat zur Folge, dass bei einem Sicherheitsvorfall und/oder einer damit verbundenen aufsichtsbehördlichen Anfrage von Unternehmensseite sehr triftige Gründe für das Weglassen einer Verschlüsselung angeführt werden müssen.

In Österreich ist dies nicht explizit gesetzlich gefordert. Eine solche Anforderung kann aber aus dem DSG 2000 abgeleitet werden und ist dringend zu empfehlen.

Sicherlich wird eine Argumentation über die wirtschaftliche Unzumutbarkeit auch bei kleineren Unternehmen oftmals nicht verfangen und akzeptiert werden. Andererseits sollten die bisherigen Erfahrungen mit den Aufsichtsbehörden nicht verschwiegen werden, denn bei solchen Fragestellungen wurde bislang meist nicht sofort sanktioniert. Dies ist aber eine trügerische Sicherheit, denn eine Verschärfung des aufsichtsbehördlichen Verhaltens ist jederzeit denkbar und die Aufforderung zur Umsetzung der gesetzlich vorgeschriebenen Maßnahmen ist sicher. Auch ist noch nicht final geklärt, ob eine fehlende Verschlüsselung unter Umständen auch abmahnfähig ist.

„Deshalb sollten erst gar keine rechtlichen Lücken beim Betrieb der Internetpräsenz zugelassen werden", betont UIMC-Geschäftsführer Dr. Jörn Voßbein und rät zu einer Verschlüsselung insbesondere von vertraulichen Datentransfers. Hierzu sind insbesondere die Kontaktformulare zu zählen. Der Einsatz von TLS-/SSL-Zertifikaten hat zudem den Vorteil, dass verschlüsselte Internetauftritte von der Suchmaschine Google höher bewertet werden, so dass auch deshalb eine komplett verschlüsselte Internetpräsenz empfehlenswert ist.

Schon gewusst?

In einem einstweiligen Verfügungsverfahren hat das Landgericht Hamburg nun mit Entscheidung vom 10.03.2016 (Az. 312 0 127/16) entschieden, dass der rechtswidrige Einsatz von Google-Analytics von Wettbewerbern abgemahnt werden kann.

Auch in Österreich ist eine Anonymisierung erforderlich, da andernfalls eine meldepflichtige Datenanwendung vorliegen kann; ferner muss das Einverständnis des Nutzers eingeholt werden (siehe auch: UIMCommunication 09/2015).

Laut den Datenschutz-Aufsichtsbhörden sind folgende Anforderungen zu erfüllen: 1. IP-Adresse anonymisieren (letzte Oktett löschen), 2. Google-Analytics-Vertrag zur Auftragsdatenverarbeitung abschließen, 3. Information mittels Datenschutzerklärung (inkl. Widerrufsrecht) sowie 4. Altdaten in Google-Analytics löschen, sofern diese rechtswidrig erhoben wurden.

UIMC® | in Datenschutz und Informationssicherheit stets gut beraten!

UIMC Dr. Vossbein GmbH & Co KG, Nützenberger Straße 119, 42115 Wuppertal

Tel.: (02 02) 2 65 74 - 0, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Tippspiel zur EM führt ohne Datenschutz-Taktik zum Eigentor

Tippspiele sind beliebt. Gerade in Zeiten von Fußballgroßereignissen, wie Welt- oder Europameisterschaften, wird gerne im Kollegen-, Freundes- oder Bekanntenkreis getippt, gefiebert und am liebsten gewonnen. Diese Beliebtheit der Tippspiele wollen viele Unternehmen nutzen. Oft heißt es dann: Mittippen und wertvolle Preise sichern. Aber schnell führt ein solches Tippspiel auf der Firmenhomepage zum datenschutzrechtlichen Eigentor. ***Dr. Jörn Voßbein bittet daher vor Start eines solchen Tippspiels, um eine gründliche Betrachtung, Beachtung und Einhaltung der bestehenden Rechtsvorschriften.***

Die Fußball-Europameisterschaft in Frankreich steht unmittelbar vor der Tür. In Kürze werden überall kleinere und größere Tippspiele mit der Chance auf attraktive Gewinne angeboten. Der Fall ist schnell erdacht: Die **Marketing**-Abteilung kommt auf die Idee, Kunden mit einem Tippspiel zur Europameisterschaft emotional noch stärker an das Unternehmen und ihre Produkte zu binden. Schnell ist die Internetplattform kicktipp.de ausgemacht, deren Tippspiel wird in die eigene Homepage eingebunden und die Kunden werden per **Newsletter** auf das EM-Tippspiel aufmerksam gemacht.

Die Teilnahmebedingungen bestimmen, dass der Gewinner sich durch Teilnahme mit der Veröffentlichung des Gewinns unter Angabe seines Namens a**uf der Unternehmens-Homepage** einverstanden erklärt. Zudem sollen die gewonnen persönlichen Daten nur im Rahmen des Gewinnspiels verwendet und nicht an Dritte weitergegeben werden.

Auf den ersten Blick scheint alles bedacht worden zu sein. Allerdings gibt es doch einige Problemfelder, die genauer betrachtet werden müssen:

- Information über das Tippspiel
- Umgang mit Anmeldedaten
- Einbindung der Partnerseite

Was es genau zu beachten gilt, finden Sie unter www.UIMC.de/communication

Neue Regeln im TMG geplant

Öffentliche WLAN-Hotspots und die Störerhaftung

Die Bundesregierung plant eine Abschaffung der Störerhaftung. Demnach sind Access-Provider, die anderen lediglich den Zugang zum Internet zur Verfügung stellen, nach dem Providerprivileg grundsätzlich nicht für das Fehlverhalten der Nutzer grundsätzlich verantwortlich.

Bitte beachten Sie: Das Gesetz ist weder verabschiedet noch in Kraft.

In-Kraft-getreten

EU-Datenschutz-Grundverordnung

Nachdem die Grundverordnung am 04.05.2016 im Amtsblatt der EU veröffentlicht wurde, trat diese am 25.05.2016 in Kraft. Sie hat ab dem **25.05.2018** Gültigkeit in allen Staaten der EU und bedarf keiner weiteren Umsetzung in nationales Recht.

Nähere Informationen erhalten Sie von Ihrem Ansprechpartner in unserem Hause und unter **www.EU-Datenschutz-Grundverordnung.info**

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- Verschlüsselte Internetseiten erhöhen Vertrauen, Sicherheit und Compliance
- Einsatz von Google Analytics
- **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: www.UIMC.de/communication

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.