UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Wie richte ich ein WLAN-Hotspot für Gäste ein, ohne für Gesetzesverstöße zu haften?

Um Kunden, Interessenten, Wirtschaftsprüfern oder anderen Gästen die Möglichkeit eines schnellen Internet-Zugangs zu bieten, gehen viele Unternehmen dazu über, einen Hotspot einzurichten. Die Gäste können dann unabhängig von Verfügbarkeit und Bandbreite des mobilen Internetzugangs E-Mails empfangen, im Internet recherchieren und ggf. auf das eigene VPN zurückgreifen. Doch wie sieht es mit der Haftung aus, wenn der Gast illegale Dinge tut (z. B. urheberrechtlich geschützte Daten herunterlädt oder denunzierende Botschaften verbreitet) und die IP-Adresse des Betreibers ermittelt wird?

Grundsätzlich ist derjenige für illegale Aktivitäten haftbar, über dessen Internetzugang diese Vorfälle geschehen sind. So müssen Nachbarn oder Eltern für den illegalen Musik-Download haften, wenn sie keine ausreichenden Maßnahmen ergriffen haben, um dies zu verhindern. Dies gilt im Übrigen auch dann, wenn der Nutzer sich beispielsweise durch Hacking Zugang verschafft hat. Anders sieht dies aber dann aus, wenn die Eltern mit den Kindern eine „Nutzungsvereinbarung" abgeschlossen haben, diese regelmäßig erneuern und zumutbare Sicherheitsmaßnahmen (z. B. Firewall-Einstellungen) ergriffen haben, die dies verhindern.

Ähnlich ist dies auch bei Unternehmen zu sehen, die Ihren Gästen einen Internetzugang anbieten wollen. Grundsätzlich steht das anbietende Unternehmen nicht in der Haftung, wenn ein Benutzer illegale Aktivitäten über Ihren Zugang begeht. Doch wenn „etwas schiefläuft", wird zunächst der Betreiber (also Sie) Ziel der Anschuldigungen sein; schließlich ist nur er über die IP nach außen ersichtlich und wird daher stets erster Ansprechpartner beziehungsweise Verdächtiger sein.

Um nicht in eine „Mitstörer-Haftung" zu geraten, empfehlen wir Ihnen Folgendes:

- Zugang nur für Berechtigte (verkehrsübliche Sicherheitsmaßnahmen durch Verschlüsselung und Zugangsbeschränkung),
- Aufstellung einer Nutzungsordnung, die der Nutzer bestätigt,
- restriktive Firewall-Einstellung (Verbot des Downloads von Musik, radikalen oder pornografischen Inhalte etc.) sowie
- Einrichtung einer DMZ zum Schutz des Unternehmensnetzwerks.

Hinsichtlich der Protokollierung gilt zu beachten, dass gemäß § 96 TKG die gespeicherten Verkehrsdaten über das Ende der Verbindung hinaus nur verwendet werden dürfen, soweit sie für andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind. Ansonsten sind die Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen. Dies bedeutet, dass Protokolle nach der Nutzung sofort gelöscht werden müssen, es sei denn, dass sie für das Erkennen, Eingrenzen oder Beseitigen von Störungen notwendig sind. Eine Datenspeicherung für etwaige Anfragen einer Strafverfolgungsbehörde ist nicht notwendig und somit nicht zulässig. Hierbei können Sie durch die angestrebten Gesetzesanpassungen noch Änderungen ergeben.

Ferner ist festzuhalten, dass die entsprechenden Daten, die durch die Benutzung erzeugt werden (Protokolle etc.), dem Fernmeldegeheimnis gemäß § 88 TKG unterliegen und gemäß § 109 TKG entsprechend zu schützen sind.

Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication

Schon gewusst?

Das Oberverwaltungsgericht Schleswig-Holstein (OVG) hat am 04.09.2014 entschieden, dass Betreiber von **Facebook-Fanpages** für Datenschutzverstöße bei der Benutzung der Seite nicht verantwortlich sind. Die UIMC informierte in der Vergangenheit über die Probleme beim Umgang mit Fanpages, Website-Plugin (z. B. **Like-Button**) etc. von sozialen Netzwerken und Lösungen dargestellt. Das OVG hat aber eine Revision zugelassen.

Fragen Sie Ihren Datenschutzbeauftragten

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 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

Wichtige Eckpunkte bei einem internationalem Datentransfer

Sobald personenbezogene Daten ins Nicht-EU/EWR-Ausland transferiert bzw. zugänglich gemacht werden, sind gesonderte Anforderungen des Datenschutzes zu beachten und (**auch konzernintern**) einer Zwei-Stufen-Prüfung vorzunehmen:

1. **Allgemeine Zulässigkeit** des Transfers
   - » Liegt eine Dienstleistung im Rahmen einer Auftragsdatenverarbeitung vor?
     Falls ja, dann ist der Auftragnehmer sorgfältig auszuwählen, ein Datenschutzvertrag abzuschließen und eine Überprüfung durchzuführen (siehe UIMCert-Kampagne). Falls nein:
   - » Liegt ein Erlaubnistatbestand vor, der einen Datentransfer legitimiert?
     Falls nein, ist der Transfer zu unterlassen.
2. Sicherstellung eines **angemessenen Datenschutzniveaus** beim Datenempfänger
   - » Ein solches Niveau ist bei einem Transfer innerhalb der EU/EWR gegeben.
   - » Bei Empfängern außerhalb der EU sind sog. **Standardverträge** der EU-Kommission abzuschließen. Alternativ können konzernintern auch sog. „Binding Corporate Rules“ genehmigt werden. Das Vorweisen eines Safe-Harbor-Certificates von US-Firmen ist grundsätzlich auch möglich, wenn auch umstritten.

Im Übrigen sind diese Anforderungen in allen EU-Staaten gleichermaßen zu beachten.

Wir empfehlen dringend, bei der Planung eines solchen Datenstranfers rechtzeitig Ihren fachkundigen Datenschutzbeauftragten einzubinden.

Weitere Empfehlungen erhalten Sie von Ihrem Ansprechpartner in der UIMC oder UIMCert.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Auszug aus bisher erschienenen Hinweisen/Tipps:

- » Fernwartung durch einen externen Dienstleister (02/2014)
- » Auditierungspflicht bei Auftragsdatenverarbeitung (09/2013)

UIMCert-Kampagne: Dienstleister-Auditierung

Sobald personenbezogene Daten durch einen Dienstleister eingesehen werden können, muss sich der Auftraggeber von der Einhaltung Ordnungsmäßigkeit überzeugen. Die UIMCert kann eine solche Auditierung auch koordinieren, indem weitere Kunden des Dienstleisters angesprochen und von einer gemeinsamen Auditierung überzeugt werden. Dies kann zu umfasssenden Kostenersparnissen führen. **Mehr unter**

uimcert.de/dienstleisterauditierung

Praxis-Workshop: Internationaler Datentransfer

In vielen **Konzernen** findet tagtäglich ein internationaler Transfer von Daten statt, weil die Mitarbeiter in Projektteams arbeiten oder eine Unternehmensgrenzen-übergreifende Aufbau- und Ablauforganisation etabliert wurde. Das Gleiche gilt beim **Outsourcing** (z. B. Cloud-Computing oder anderer internetbasierter Tools).

Diskutieren Sie über die rechtlichen Anforderungen und Lösungsmöglichkeiten mit einem erfahren Berater!

Wuppertal, 15.10.2014

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

- ☐ Was tun, wenn ein Gäste-WLAN-Hotspot installiert werden soll?
- ☐ Gefahren bei der Nutzung eines öffentlichen Hotspots
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

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