Gemeinsame Datenschutzbeauftragte der Hamburger Hochschulen UHH, HfMT, HFBK, HCU, TUHH & der SUB

Weitergabe von Passworten

gDSB-Info, 24.03.2011

Aus gegebener Veranlassung weisen wir darauf hin, dass die **Weitergabe von Passworten unzulässig** ist. Die Weitergabe stellt einen gravierenden Verstoß gegen das Datenschutzrecht dar. Mit Blick auf das Hamburgische Datenschutzgesetz (HmbDSG) liegt ein Verstoß gegen das Datengeheimnis (§ 7 HmbDSG) vor. Ferner ist die Vertraulichkeit (nur Befugte dürfen die personenbezogenen Daten zur Kenntnis nehmen), die Authentizität (die personenbezogenen Daten können ihrem Ursprung zugeordnet werden) und die Revisionsfähigkeit (es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat) verletzt (§ 8 Abs. 2 HmbDSG).

Die Weitergabe eines vertraulichen Passwortes stellt zumindest eine Ordnungswidrigkeit nach § 33 HmbDSG dar, die mit einer Geldbuße bis zu 25.000,- € geahndet werden kann. Zuständig für die Einleitung eines entsprechenden Verfahrens ist nach dem Verwaltungsverfahrensgesetz die jeweilige Dienststellenleitung. Weitere arbeitsrechtliche Maßnahmen können unabhängig von den datenschutzrechtlichen Grundlagen eingeleitet werden. Zahlreiche Gerichtsurteile belegen, dass auch fristlose Kündigungen gerechtfertigt sein können. Dies gilt selbstverständlich auch für den Fall, dass Mitarbeiterinnen und Mitarbeiter von Vorgesetzten, Kolleginnen/Kollegen oder anderen Dritten gedrängt werden, ihr persönliches Passwort herauszugeben.

Kein Grund rechtfertigt ein solches Vorgehen! Wir empfehlen Ihnen in einem solchen Fall, Ihre Personalvertretung oder uns als Datenschutzbeauftragte anzusprechen.

Die Geschäftsprozesse sind vor einer Inbetriebnahme von IT-Verfahren so auszugestalten, dass entsprechende Stellvertretungsregelungen (Email-/Groupware-Stellvertreter, Gruppenlaufwerke, etc.) eingerichtet sind. Auch für absolute Notfälle (plötzliche Krankheit, etc.) sollten geregelte Verfahren (z.B. Passwortrücksetzung durch die IT-Administration) etabliert und dokumentiert sein.

Zahlreichen Hochschul-/Verwaltungs-Richtlinien belegen die datenschutzrechtlichen Grundlagen. Beispielsweise führt die PC-Richtlinie der FHH in Ziff. 2.2 aus:

> ***Organisatorische und technische Maßnahmen***
> *…*
> *(6) Rechner sind entsprechend der geltenden Passwort-RL vor unbefugten Zugriffen zu schützen. Nach einer ordnungsgemäßen Abmeldung sind ggf. weitere technische und organisatorische Sicherheitsvorkehrungen zu treffen. Räume, in denen Endgeräte aufgestellt sind, sind bei Verlassen abzuschließen.*

Die zitierte Passwort-Richtlinie der FHH, die für alle Dienststellen Gültigkeit hat, konkretisiert in Ziffer 2

> ***Pflichten der Benutzer***
> *(1) Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt oder unverschlüsselt auf Rechnern gespeichert werden.*

Eine Studie des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V., kurz BITKOM e.V., zeigt einen recht lockeren Umgang im Zusammenhang mit der Weitergabe von vertraulichen Passworten auf (siehe u.a. Link).

Die Weitergabe von Passworten ist kein Kavaliersdelikt!

Bernd Uderstadt
Referent der gemeinsamen Datenschutzbeauftragten der Hambuger Hochschulen UHH, HfMT, HFBK, HCU & TUHH / Datenschutzbeauftragter der SUB

Links:

http://www.bitkom.org/66830_64114.aspx

http://www.anwalt24.de/beitraege-news/fachartikel/weitergabe-von-passwort-rechtfertigt-fristlose-kuendigung

---

Für Rückfragen und weitere Informationen wenden Sie sich bitte an:

Staats- und Universitätsbibliothek Hamburg Carl von Ossietzky
Gemeinsame Datenschutzbeauftragte der Hamburger Hochschulen
U H H, H f M T, H F B K, H C U, T U H H & der S U B
Gabriele Beger & Bernd Uderstadt (DSB der SUB)
Von-Melle-Park 3, 20146 Hamburg
✆ +49 40 42838-5801
🖷 +49 40 42838-3352
✉ datenschutz@sub.uni-hamburg.de
✉ bernd.uderstadt@sub.hamburg.de