Personalisierte Kennungen und Passworte

Die Vergabe personalisierter Kennungen mittels User-ID und Passwort - zum Schutz von dienstlichen PCs, Laptops, Mobile Devices, Anwendungen, Datenbanken, Fachverfahren , elektronischen Postfächern, persönlichen Ordnern, usw. - stellt typischer Weise eine von mehreren Maßnahmen dar, um unberechtigte Zugriffe auf die verarbeiteten personenbezogenen Daten zu verhindern und damit die notwendige Informationssicherheit der uns anvertrauten Datenbestände und Informationen zu gewährleisten.

Vielfach werden in heutiger Zeit verschiedene Fachanwendungen einschließlich der Zugriffe auf persönliche oder gar private Verzeichnisse oder Dateien (*) über zentrale, personalisierte Kennungen geschützt (Single-Sign-On (SSO), IDMS, Active Directory). Technisch verbirgt sich dahinter oft ein differenziertes, feingranulares Rechte- und Rollenkonzept ... personalisiert für die jeweilige berechtigte Person.

(*) = vgl. 93er Vereinbarung zur Bürokommunikation für Beschäftigte).

Das für die öffentlichen Hamburger Hochschulen, Universitäten und Bibliotheken einschlägige Hamburgische Datenschutzgesetz (HmbDSG) formuliert hierzu im Allgemeinen in § 1 HmbDSG:

> *Dieses Gesetz regelt die Verarbeitung personenbezogener Daten durch öffentliche Stellen, um das Recht einer jeden Person zu schützen, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind.*

Die zu ergreifenden **t**echnisch-**o**rganisatorischen **M**aßnahmen (TOM) sind, in Abhängigkeit vom Schutzbedarf der verarbeitenden personenbezogenen Daten, aus § 8 HmbDSG abzuleiten:

> *„Werden personenbezogene Daten automatisiert verarbeitet, sind technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass*
>
> 1. *nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Vertraulichkeit),*
> 2. *die personenbezogenen Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (Integrität),*

3. *die personenbezogenen Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),*
4. *die personenbezogenen Daten ihrem Ursprung zugeordnet werden können (Authentizität),*
5. *festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit).“*

Daraus kann unmittelbar die Verpflichtung für jede zugriffsberechtigte Person eingefordert werden, Passworte geheim zu halten und nicht an Dritte weiterzugeben – auch nicht im Ausnahmefall (bedenken Sie dabei den Umfang der erteilten Rechte und Rollen und ggf. die Zugriffsmöglichkeiten auf persönliche Dateien). Zudem ist es den IKT-Abteilungen und Rechenzentren in aller Regel möglich, berechtigten Vertreterinnen bzw. Vertretern eine personalisierte, eigene Kennung für die jeweilige Anwendung zu erteilen.

Die Weitergabe von personalisierten Kennungen stellt - im Zusammenhang mit der Verarbeitung personenbezogener Daten - einen gravierenden Verstoß gegen das geltende Datenschutzrecht dar.

Darüber hinaus verstoßen Sie in einem solchen Fall zudem gegen Nutzungsordnungen, Sicherheits-Richtlinien und arbeitsrechtliche Regelungen Ihrer Arbeitgeberin.
Mit Blick auf das Hamburgische Datenschutzgesetz (HmbDSG) liegt ferner ein Verstoß gegen das Datengeheimnis (vgl. § 7 HmbDSG) vor:

> *Denjenigen Personen, die bei den in § 2 Absatz 1 Satz 1 HmbDSG genannten Stellen oder ihren auftragnehmenden Stellen dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, insbesondere bekannt zu geben oder zugänglich zu machen. Dieses Verbot besteht auch nach Beendigung der Tätigkeit fort.*

Ferner ist die Vertraulichkeit, die Authentizität und die Revisionsfähigkeit nach § 8 Abs. 2 HmbDSG verletzt.
Beachten Sie, dass sich der Gesetzgeber beim Datengeheimnis ausdrücklich nicht auf Beschäftigte beschränkt, sondern jede Person in die Pflicht nimmt, die einen geschäftlichen bzw. dienstlichen Zugang zu personenbezogenen Daten hat. Dabei fordert das HmbDSG im Gegensatz zu anderen Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz (BDSG) keine schriftliche Verpflichtung ein. Allerdings sind Beschäftigte der Universität Hamburg und der HafenCity Universität Hamburg

schriftlich auf das Datengeheimnis zu verpflichten sofern sie Personaldaten verarbeiten (aufgrund von Dienstvereinbarungen der Präsidien mit den Personalvertretungsgremien).

Die Weitergabe eines vertraulichen, personalisierten Passwortes kann als Ordnungswidrigkeit nach § 33 HmbDSG mit einer Geldbuße bis zu 25.000,- € geahndet werden. Im Einzelfall kann der Verstoß auch strafbewährt sein.
Die mögliche Einleitung eines entsprechenden Verfahrens obliegt nach dem Hamburgischen Verwaltungsverfahrensgesetz (HmbVwVfG) nicht dem Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) sondern der Leitung der verantwortlichen Daten verarbeitenden Stelle (Präsidium, Direktorium). Weitere Maßnahmen, z.B. arbeitsrechtlicher Art, können unabhängig von den datenschutzrechtlichen Grundlagen eingeleitet werden. Zahlreiche Gerichtsurteile belegen, dass in der Vergangenheit auch fristlose Kündigungen ausgesprochen worden sind.

Dies gilt selbstverständlich auch für den Fall, dass Mitarbeiterinnen und Mitarbeiter von Vorgesetzten, Kolleginnen / Kollegen oder anderen Dritten gedrängt werden, ihr persönliches Passwort herauszugeben.

Abgesehen von einer wohl eher theoretischen Gefahr für Leib und Leben von Betroffenen rechtfertigt kein Grund ein solches Vorgehen!

Wird Ihnen ein solcher Fall bekannt oder sind Sie persönlich betroffen, so empfehle ich Ihnen, sich umgehend an Ihre Personalvertretung, Ihre/Ihren Informationssicherheitsbeauftragte/n (InSiBe), den Hamburgischen Beauftragten für Datenschutz (HmbBfDI) oder an mich als behördlichen Datenschutzbeauftragten zu wenden.

Die Geschäftsprozesse sind vor einer Inbetriebnahme von IT-Verfahren so auszugestalten, dass entsprechende Stellvertretungsregelungen (Email-/Groupware-Stellvertreter, Funktionspostfächer, Gruppenlaufwerke, etc.) eingerichtet sind. Auch für absolute Notfälle (längere Krankheit, etc.) sollten geregelte Verfahren (administrative Schaltung von Abwesenheitshinweisen, Mail-Weiterleitung, ggf. auch eine datenschutzgerechte 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.

Ähnliche Vorgaben gelten auch in Ihren Dienststellen. Beispielhaft seien an dieser Stelle die Informationssicherheits-Leitlinien (IS-LL) von UHH und TUHH sowie die davon abgeleiteten konkreten Regelungen und Policies genannt.
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. Links):

- https://www.bitkom.org/Presse/Presseinformation/Stress-mit-der-Passwort-Flut.html
- http://www.anwalt24.de/beitraege-news/fachartikel/weitergabe-von-passwort-rechtfertigt-fristlose-kuendigung

Die Weitergabe von personalisierten Passworten ist kein Kavaliersdelikt!

Kontakt:

Bernd Uderstadt
Datenschutzbeauftragter (DSB) der Universität Hamburg (UHH)
sowie externer DSB der Hmb. Hochschulen HfMT, HFBK, HCU, TUHH
und der Staats- und Universitätsbibliothek Hamburg (SUB)

Universität Hamburg, Stabsstelle Recht, DSB (UHH/R16)
Mittelweg 177 (Rm. N 0051) * D-20148 Hamburg
Telefon: +49 40 42838-2957
E-Mail: datenschutz [at] uni-hamburg.de
Internet: https://www.hh-datenschutz.de

//

Versionierung und Gültigkeit

Dok.: 161020_DSB--Pers_Kennungen_und_Passworte.docx

Version	Datum	von	Beschreibung der Änderung(en)
1.0-1.3	2011-2014	DS-Ref/gDSB (SUB)	ohne Versionierung
1.4	28.10.2015	DSB (KoopDS)	Layout, allg. inhaltl. Anpassungen
1.5	22.07.2016	DSB (KoopDS)	Löschung CC-Lizenzhinweis
1.6	20.10.2016	DSB (KoopDS)	Anpassung Kommunikationsdaten
Gültig bis:	**24.05.2018**		