Ein weites Feld!

Das zweite Gebot: Die Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte DV-Anlagen benutzen können. Es geht dabei um die Frage der Identifikation und der anschließenden Authentifikation. Die Zugangskontrolle hat auch das Ziel, einen externen Zugang zu DV-Anlagen, etwa aus dem Internet, zu unterbinden. Ein schier grenzenloses Kontrollfeld für den Datenschutzbeauftragten!

Nach dem ersten Gebot der Zutrittskontrolle (siehe Ausgabe September 2010) führt die Anlage zu § 9 BDSG als zweites Gebot die Zugangskontrolle auf. Sie soll „verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können“.

Definition der Zugangskontrolle

Mit Zugangskontrolle ist die Verhinderung einer Nutzung von Anlagen gemeint, mit denen personenbezogene Daten verarbeitet werden. Es geht also darum, dass nur befugte Personen Zugang zu DV-Anlagen erhalten.

Vorsicht, Verwechslungsgefahr

Oft wird die Zugangskontrolle allerdings verwechselt. Die Kontrolle, dass befugte Personen DV-Anlagen nur im Rahmen ihrer Berechtigungen nutzen, ist Aufgabe der Zugriffskontrolle.

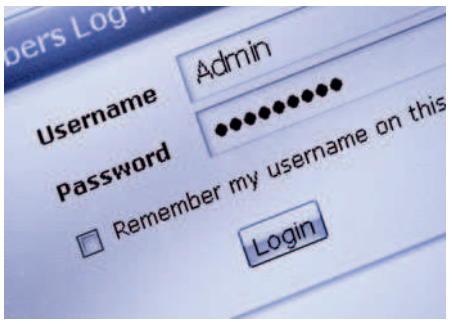
Keine Passwörter „verleihen“!

Der zu kontrollierende Bereich aus Nr. 2 der Anlage zu § 9 BDSG zur Zugangskontrolle beginnt beim Einschalten der Datenverarbeitungsanlage und beim Hochfahren des Systems.

Kern einer korrekten Datensicherungsmaßnahme ist es, unberechtigte Zugriffe zu verhindern. Jeder Benutzer muss sich daher für den Zugang auf IT-Systeme identifizieren und authentifizieren. Das oft praktizierte „Ausleihen“ von Benutzeraccounts, z.B. während der Urlaubsvertretung, muss grundsätzlich verboten werden.

Prüfen Sie die Passwortqualität

Kontrollieren Sie als Datenschutzbeauftragter die betrieblichen Regelungen zur Passwortvergabe. Wer darf Kennwörter vergeben oder ändern? Prüfen Sie auch gleich die Qualität der Kennwörter wie Passwortlänge, Verwendung von Ziffern und Sonderzeichen, Anwendung der Groß-/Kleinschreibung, regelmäßiger Passwortwechsel sowie Sperrung bei wiederholter Fehleingabe.



Ein wichtiges Instrument der Zugangskontrolle sind Passwörter

Zudem sollten Benutzerinfos über den korrekten Umgang mit Passwörtern existieren. Wichtig: Die Weitergabe von Passwörtern an Kollegen darf keinesfalls erlaubt sein!

Geben Sie mobile Geräte stets nur verschlüsselt heraus

Das Gebot der Zugangskontrolle ist z.B. auch für den sicheren Zugang zu mobilen Geräten anzuwenden. Notebooks, auf denen personenbezogene Daten gespeichert sind, sollten nur noch mit aktiver Datenverschlüsselung an Nutzer ausgegeben werden.

Sofern es sich auf den Mobilgeräten gar um Daten nach § 42a BDSG handelt, ist ein wirksames Data-Loss-Prevention-(DLP-)Verfahren zwingend.

Sind sichere Übertragungstechniken im Einsatz?

Das Thema sicherer Übertragungstechniken in Verbindung mit der Zugangskontrolle ist ein weites Feld. Prüfen Sie doch mal in Ihrem Unternehmen, welche Datenkategorien und -felder ungeschützt transferiert werden!

E-Mails mit Mitarbeiterdaten und Bankinformationen werden noch zu oft ohne jegliche Sicherungsmaßnahmen an den Steuerberater oder externe Unternehmen zur Personalabrechnung gesendet. Dass dabei der Transfer über eine „Postkarte“ erfolgt, sollte inzwischen hinlänglich bekannt sein.

Schutz vor Viren & Co.

Zum Stand der Technik in der Datenverarbeitung ist ein aktiver Virenscanner mittlerweile unerlässlich. Dass hierbei auch das Thema Zugangskontrolle tangiert wird, sollte der Datenschutzbeauftragte bedenken. Denn schleusen infizierte Dateien über ungesicherte Systeme schädlichen Code ein, untergräbt das die Bemühungen, zu verhindern, dass Unbefugte die Datenverarbeitungssysteme nutzen.

Abschottung nach außen

Eine Firewall dient der Beschränkung sowie der Regelung der Netzwerkzugriffe, um den unberechtigten Zugriff von außen auf Unternehmenssysteme zu verhindern. Doch Vorsicht, die Funktion einer Firewall besteht nicht darin, Angriffe zu erkennen!

Bildschirmsperre immer aktivieren

Ein so lapidares Thema wie eine automatische Bildschirmsperre bei längerem Inaktivsein sollte eine Selbstverständlichkeit sein, um neugierige Blicke zu verhindern.

Eine Tastenkombination oder ein Mausklick vor Verlassen des Arbeitsplatzes schützt vertrauliche Informationen und wahrt die Zugangskontrolle. Dass die Reaktivierung des Bildschirms nur per Kennwort durchgeführt werden darf, versteht sich von selbst.

(Nicht) offen für Ausgeschiedene

Scheiden Mitarbeiter aus dem Unternehmen aus, wird des Öfteren die Deaktivierung der Zugangsberechtigungen vernachlässigt. Eine zeitnahe Sperrung der Befugnisse ist jedoch zwingend notwendig!

Berechtigungen kontrollieren

Außerdem sollte man regelmäßig die Gültigkeit von Berechtigungen kontrollieren. Bisweilen werden im Rahmen von Urlaubsvertretungen erweiterte Zugriffsrechte erteilt. Auf die Rücknahme nach Beendigung der Vertretungsphase wird die Administration in den seltensten Fällen aufmerksam gemacht.

Maßnahmen-Checkliste

Die Checkliste der notwendigen Kontroll- und Dokumentationsmaßnahmen in diesem Beitrag ist selbstverständlich nicht vollständig. Prüfen und ergänzen Sie die Liste entsprechend Ihren betrieblichen Erfordernissen.

Hermann Keck

Regelung zur Zugangskontrolle	Erfüllt?	Bemerkung
Identifikation über eindeutige User-ID		
Authentifizierung über Passwort		
Sind schriftliche Regelungen zum Passwortgebrauch und zur Passwortgestaltung vorhanden?		
Kontosperre bei fehlerhaften Zugangsversuchen		
Wird ein regelmäßiger Passwort-Wechsel erzwungen?		
Werden ausgeschiedene Mitarbeiter umgehend gesperrt?		
Wurden die Benutzer über den korrekten Umgang mit Benutzeraccount und Passwörtern unterrichtet?		
Ist die Vergabe bzw. Löschung/Rücknahme der Zugangsberechtigungen schriftlich dokumentiert?		
Wird die Gültigkeit von Berechtigungen regelmäßig kontrolliert (mind. 1x jährlich)?		
Einsatz sicherer Übertragungstechniken (VPN-Tunnel)		
Viren-Scanner für Server und Arbeitsplatzrechner?		
Abschottung nach außen (Firewalls, Verschlüsselung)		
Automatische/manuelle Rechnersperre bei vorübergehender Abwesenheit (kennwortgeschützter Bildschirmschoner)?		
Werden personenbezogene Daten über ungesicherte Transportwege versandt?		
Werden die Zugänge zu den Datenverarbeitungssystemen protokolliert (Log-Protokolle)?		
Werden Logprotokolle aus der Zugangskontrolle nach Unregelmäßigkeiten ausgewertet?		
Sind interne Netze gegen unberechtigte Zugriffe von innen geschützt?		
Datenverschlüsselung von mobilen Endgeräten aktiv?		
Sind private Speichermedien verboten?		
Sind Verteilerschränke abgeschlossen?		
Sie die WLAN-Verbindungen abgesichert?		
Sonstige Maßnahmen?		

Checkliste Zugangskontrolle: Wie wird verhindert, dass Unbefugte Datenverarbeitungssysteme nutzen? Abonnenten finden diese Checkliste zum kostenlosen Download unter www.datenschutz-praxis.de/fachwissen/vorlagen/checklisten.