Kiesche/Wilke, BSI-Grundschutz-Kataloge: Vielfältiger Nutzen auch für Personalräte,
veröffentlicht in: Der Personalrat 11/2007, 455ff

Einführung

Auch im öffentlichen Bereich ist der Einsatz von Informationstechnik (IT) immer weniger aus der alltäglichen Arbeit wegzudenken. Viele Arbeitsprozesse sind elektronisch gesteuert, ebenso die Erhebung, Verarbeitung und Übermittlung besonders von personenbezogenen Daten. Die Integrität, Vertraulichkeit und Verfügbarkeit von Daten ist ein wichtiges Ziel von Unternehmen und Verwaltung. Wirtschaft und öffentliche Verwaltung werden immer abhängiger von einer funktionierenden Informationstechnik (IT) und benötigen von daher umfassende Dienstleistungen im Bereich der IT-Sicherheit.
Denn die Gefahr massiver wirtschaftlicher Schäden ist immer bedrohlicher. Enorme Zunahme von Spam, Attacken mit Computerschädlingen wie Trojanische Pferde, Würmer und neuerdings Spionagesoftware und Hackerangriffe: alles ist an der Tagesordnung. Zudem sind leider in der Praxis die folgenden Gefährdungen zu beobachten: völlig ungesicherte drahtlose Netze, unbedachtes Weiterreichen von Passwörtern und schludriger Umgang damit, mangelhafte Schulung von Administratoren und Anwendern, schlechte Wartung von IT-Systemen, Schadfunktionen in Dateianhängen empfangener E-Mails, unbeaufsichtigtes Arbeiten der Administratoren mit Systemprivilegien und vieles mehr. Hier liegt nach wie vor vieles im Argen.
Das Bundesamt für Informationstechnik in Bonn Bad Godesberg (im folgenden BSI) bietet seit 1991 zur Abhilfe dieser Gefährdungen Grundlagenarbeit im Bereich der IT-Sicherheit an. Das Bundesamt hat den IT-Grundschutz seit 1995 als De-Facto-Standard durchgesetzt. 1995/6 entstand nämlich das **IT-Grundschutzhandbuch** in Zusammenarbeit mit einigen Aufsichtsbehörden, das inzwischen anders aufgegliedert und benannt worden ist. In den IT-Grundschutz-Katalogen und BSI-Standards existiert inzwischen eine gewaltige Fülle von Informationen, Methoden, Checklisten und Anleitungen, wie die IT-Sicherheit bei IT-Anwendungen und IT-Systemen zu verbessern ist.
Im folgenden soll der Auftrag des BSI und die Dienstleistungen des BSI hinsichtlich IT-Sicherheit im Einzelnen dargestellt, die IT-Grundschutz-Konzeption anhand eines ausgewählten IT-Systems verdeutlicht und vor allem ihr Nutzen für Personalräte erörtert werden. Personalräte nutzen leider, so unsere Beobachtung in Beratungen und Schulungen, bislang noch zu wenig die Grundschutzkataloge für ihre Arbeit bei der Mitgestaltung von technischen Kontrolleinrichtungen und der Überwachung eines funktionierenden Datenschutzmanagements. Von daher sind von uns die folgenden Fragen zu beantworten: Wie können Personalräte die Grundschutz-Kataloge nutzen? Wo sind ihre Beteiligungsrechte betroffen? Wie können sie ihre Rechte für mehr Datenschutz und Datensicherheit nutzen und sich dabei auf diese „Bibel der IT-Sicherheit“ berufen?

1. Das BSI und sein Auftrag

Das BSI[1] ist das Kompetenzzentrum für Informationssicherheit in Deutschland geworden; es ist dem Bundesinnenministerium unterstellt. Der Auftrag des BSI ist im „Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz vom 17. Dezember 1990, BGBL: I S.2834) festgelegt; das Gesetz trat 1991 in Kraft und ist seither im Wesentlichen unverändert geblieben. Inzwischen arbeiten über 450 Experten im BSI mit dem Ziel, die IT-Sicherheit in Deutschland zu erhöhen.

[1] Informationen zum BSI sind zu finden unter: www.bsi.bund.de Viele Begriffe, die hier im Aufsatz verwendet werden, sind im Glossar unter www.bsi.de/gshb definiert.

Das BSI wendet sich mit seinen Dienstleistungen an Anwender, Vertreiber und Hersteller von Informationstechnik, und als öffentliche Einrichtung sicherlich in erster Linie an die öffentlichen Verwaltungen in Bund, Länder und Kommunen. Das BSI versteht sich selbst als der zentrale IT-Dienstleister für den Bund, besonders im Bereich von E-Government-Strategien[2] des Bundes.
Zweck des BSI ist die Förderung der Sicherheit in der Informationstechnik. IT-Sicherheit oder Datensicherheit meint den Schutz der Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit[3], Verfügbarkeit[4] und Integrität[5]**.** Zusätzlich müssen im Rahmen der Datensicherheit auch Authentizität[6] und Revisionsfähigkeit der Daten verwirklicht werden. Diese Ziele sind, ausgerichtet am Schutzbedarf der Daten[7], durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.
Das BSI berät, forscht und informiert zu Sicherheitsrisiken und entwickelt Sicherheitsvorkehrungen. Im BSI-Errichtungsgesetz, BSI-Leitbild und in Kurzinformationen werden die Aufgaben des BSI wie folgt beschrieben:

- Informationen über Gefährdungen und Gegenmaßnahmen in Handbüchern, Faltblättern, Broschüren einschließlich Durchführung von Kongressen, Teilnahme an Messen und Versand von Newsletter,
- Untersuchung von Sicherheitsrisiken bei der Anwendung von Informationstechnik,
- Entwicklung von Sicherheitsverfahren und Geräten für die IT-Sicherheit,
- Verfahren für Prüfung und Bewertung von IT-Systemen,
- Vergabe von Sicherheitszertifikaten,
- Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes,
- Unterstützung der Polizei und der Verfassungsschutzbehörden,
- Beratung der Hersteller, Anwender und Vertreiber in allen Fragen der Sicherheit von IT und
- Akkreditierung von IT-Sicherheitsdienstleistern.

Diesbezügliche Handlungsanleitungen finden sich u.a. in IT-Grundschutz-Katalogen, BSI-Standards zum Sicherheitsmanagement und zur Vorgehensweise, Jahresberichten, Kurzinformationen und in einem benutzerfreundlichen Leitfaden zum IT-Sicherheitsmanagement.

2. IT-Grundschutz: Idee, Konzeption und Hilfsmittel

Grundidee des IT-Grundschutzes ist es, die IT-Sicherheit ständig kontinuierlich zu verbessern und langfristig in Organisationen ein funktionierendes IT-Sicherheitsmanagement aufzubauen, besonders auch dann wenn kein großes Budget vorhanden ist.
Von daher legt das BSI großen Wert auf ein nach dem Grundschutzstufenkonzept entwickeltes IT-Sicherheitskonzept, dessen arbeitsökonomische Erstellung und auf Vermeidung umständlicher bzw. nicht erforderlicher Sicherheitsmaßnahmen. Ziel ist es, angemessene Kon-

---

[2] Kiper, M., E-Government Aufsatz im Personalrat
[3] Vertraulichkeit ist der Schutz vor unbefugter Preisgabe. Diese Begriffserklärung und alle folgenden sind wenn immer möglich, den Veröffentlichung des BSI entnommen.
[4] Verfügbarkeit: Dem Benutzer stehen Dienstleistungen, Funktionen eines It-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.
[5] Integrität bedeutet, dass die Daten vollständig und unverändert sind.
[6] **Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.**
[7] Vgl. zu den Schutzstufen BSI Standard 100-2 bzw. landesspezifische Regelungen zum Datenschutz.

zepte und Maßnahmen zu entwickeln und deren kostengünstige und möglichst praxiserprobte Umsetzung zu betreiben.
Was bietet das BSI an Dienstleistungen? In den online-verfügbaren und sehr gebrauchstauglichen Handbüchern und Katalogen findet sich eine vollständige Anleitung zur Verwirklichung eines IT-Sicherheitsmanagement in Unternehmen und Verwaltung, die zudem ständig aufgrund von Anwenderbefragungen fortgeschrieben wird. Die Vorgehensweise nach der Konzeption des IT-Grundschutzes findet sich seit 2005 in den BSI-Standards. Zu unterscheiden sind:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: Vorgehensweise nach IT-Grundschutz
- BSI-Standard 100-3: Risikoanalyse nach IT-Grundschutz.

Der BSI-Standard 100-2 beschreibt die IT-Grundschutz-Vorgehensweise und erklärt schrittweise notwendige Bausteine zur Erstellung eines IT-Sicherheitskonzeptes. Hierdurch erfolgt eine Operationalisierung von ISO-Standards zur IT-Sicherheit[8]. Im folgenden sollen ausgewählte Hinweise zum ganzheitlichen Vorgehen nach IT-Grundschutz referiert werden, die aus Personalratssicht von besonderer Bedeutung sind.
IT-Sicherheitsaspekte sollten von Beginn an berücksichtigt werden. Dies kann Kosten sparen helfen. Bei der Entscheidung, welches IT-System gekauft und eingesetzt werden soll, sollte zunächst die Frage nach der erforderlichen Funktionalität geklärt werden. Auf unnötige Funktionen sollte verzichtet werden, um insgesamt den Aufwand für Sicherheitsvorkehrungen zu senken. Eine exakte Klärung der gesetzlichen Rahmendingungen und zusätzlich die Festlegung von sind auch für Personalräte unerlässliche Voraussetzungen für Wahrnehmung ihrer Mitbestimmungsrechte.
Für eine umfassende Verwirklichung von Datenschutz und Datensicherheit sind zusätzlich der Schutzbedarf festzustellen, Schadensfälle zu klassifizieren, Richtlinien und Maßnahmen zu definieren, ein Handlungsplan zu erstellen und die technische Infrastruktur bereit zu stellen. Je höher der Schutzbedarf anzusiedeln ist, desto mehr Aufwand sollte in die Maßnahmen zur IT-Sicherheit gesteckt werden. Alle Schritte, Schadensfälle, Maßnahmen und Richtlinien sind zu dokumentieren. Von Beginn an sind Kontrollmechanismen einzubauen. Auch hievon profitieren Personalräte, wenn sie die Einhaltung der Dienstvereinbarungen zu technischen Kontrollsystemen überwachen.
Besonders spannend für Personalräte ist der Hinweis[9], dass ein restriktives Berechtigungskonzept bei jedem IT-System und jeder IT-Anwendung erforderlich ist. Nach dem „Need-to-Know-Prinzip“ sollte jeder Benutzer und jeder Administrator nur auf die Datenbestände oder Programme zugreifen können, die er für seine tägliche Arbeit benötigt. In der Praxis wird eine eng begrenzte Rechtevergabe oftmals missachtet. Ein umfassender Zugriffsschutz aufgrund von § 9 BDSG samt Anlage muss hiermit verwirklicht werden.[10]
Allen Systembenutzern müssen z.B. in ERP-Systemen[11] Rollen und Profile aufgrund ihrer Aufgabenstellung zugeordnet werden und dürfen kein Sammelsurium an Berechtigungen erhalten. Systemadministratoren sollten je nach Größe der IT-Abteilung Berechtigungen für Rollen zugewiesen bekommen. Dies geschieht durchaus auch zu ihren Schutz. Denn dies ist die Erfahrung der Autoren des IT-Grundschutzes: Zu weit reichende Berechtigungen können versehentlich, durch Unkenntnis oder beabsichtigt missbraucht werden.

---

[8] ISO-Standards 13335, 17799 und 2701
[9] Vgl. Leitfaden, S. 22
[10] Vgl. Wedde, § 9 RdNr 54, in: Däubler, Klebe, Wedde, Weichert, Bundesdatenschutzgesetz. Basiskommentar zum BDSG., 2. Auflage, 2007, hier S. 257
[11] ERP-Systeme (Enterprise resource Planning): IT-Systeme, die alle Funktionsbereiche eines Unternehmens erfassen.

Die **IT-Grundschutz-Kataloge** bieten zusätzlich zu den BSI-Standards weitergehend eine Basis für die inhaltliche und methodische Ausgestaltung eines angemessenen Schutzniveaus in der Dienststelle. Sie können aufgrund ihres modularen Aufbaus als technischer Leitfaden und Ratgeber für verschiedenste Sicherheitsfragestellungen genutzt werden. Sie berücksichtigen immer auch die Bereiche Infrastruktur Organisation, Personal, Technik und Notfallvorsorge mit.
Die IT-Grundschutz-Kataloge geben inhaltliche Unterstützung für ein zielgerichtetes Vorgehen, sind zudem eine Basis für umfassende Risikobewertung und für eine Überprüfung der bisherigen IT-Sicherheit und schlussendlich die Grundlage für die Implementierung einer angemessenen IT-Sicherheit und eines durchdachten IT-Sicherheitsmanagement.
Zusätzlich werden typische IT-Systeme und Anwendungen hinsichtlich Gefährdungen und Gegenmaßnahmen dargestellt, u.a. Spam, RFID, Telearbeit, VoIP (Voice over IP[12]), SAP-Systeme und Sicherheitsgateways. Bei allen IT-Anwendungen und IT-Systemen müssen, so die Botschaft des IT-Grundschutzes, immer technische, organisatorische, personelle und baulich-physische Maßnahmen kombiniert werden. Für typische IT-Anwendungen und IT-systeme werden praxiserprobte Standard-Sicherheitsmaßnahmen detailliert beschrieben, die nach dem aktuellen Stand de Technik umzusetzen sind. Dabei wird auch und nur das erforderliche technische Wissen vermittelt.
Die Struktur der Bausteine lässt sich wie folgt beschreiben:

- Baustein 1 beschreibt übergreifende IT-Sicherheitsaspekte wie z. B. Personal und Organisation.
- Baustein 2 berücksichtigt baulich-technische Gegebenheiten (u.a. Serverraum, Gebäude, häuslicher Telearbeitsplatz).
- Baustein 3 beschäftigt sich mit typischen IT-Systemen, z. B. mit Unix-Systemen und tragbaren Personal Computern.
- Baustein 4 stellt Vernetzungsaspekte der IT-Systeme wie z.B. Netz- und Systemmanagement dar.
- Baustein 5 hat die Thematik der typischen IT-Anwendungen wie z.B. E-Mail, WWW-Server und Datenbanken.

Die jeweilige Thematik wird jeweils kurz beschrieben und verweist auf mögliche Gefährdungen und relevante Sicherheitsmaßnahmen.

3. IT-Grundschutz am Beispiel von SAP

Anhand eines IT-Systems soll der Nutzwert der IT-Grundschutz-Kataloge für die Arbeit der Personalräte aufgezeigt werden. Dabei handelt es sich um das SAP-System. Es ist eine betriebswirtschaftliche Software, die umfassend alle betriebswirtschaftlichen Funktionsbereiche eines Unternehmens oder einer Verwaltung abdeckt. Dieses ERP-System als Marktführer verarbeitet somit auch vertrauliche und personenbezogene Daten. Seine Grundfunktionalitäten und die SAP-Grundbegriffe werden in den IT-Grundschutz-Katalogen kurz beschrieben[13].
Zu Recht wird darauf verwiesen, dass mit SAP-System nicht mehr eindeutig eine bestimmte Konfiguration gemeint sein kann. Es gibt nicht mehr nur eine Konstellation oder Konfiguration von Komponenten des Systems. Diese Software verwirklicht immer stärker die Idee einer serviceorientierten Softwarearchitektur[14], die für beliebe betriebliche Zwecke Funktionalitä-

[12] Voice over IP: Telefonieren über das Internet. Im Gegensatz zur leitungsgebundenen Vermittlung werden bei VoIP-Systemen die Gespräche über die paketorientierte Vermittlung übertragen.
[13] Vgl. M 3.53 Darstellung der Komponenten und Fachbegriffe wie z. B. Transaktionen und Tabellen (M steht für Maßnahme).
[14] Bieler, SOA – Technik für flexible und offene IKT-Landschaften; Computer und Arbeit 4/2007, S. 20-23.

ten oder Services bereitstellt. Das Sicherheitskonzept wird von daher nicht auf ein bestimmtes SAP-System bezogen entwickelt und auch nicht auf ein bestimmtes Modul wie die Personalwirtschaft HCM[15]. Wie hilft der IT-Grundschutz den SAP-Anwendern? Es werden Hinweise für Gefährdungen im Bereich der neuen Basiskomponente NetWeaver Application Server gegeben. Es finden sich nützliche Verweise auf SAP-Dokumente wie Sicherheitsleitfäden und Datenschutzleitfaden. Dabei soll die SAP-eigene Dokumentation um beachtenswerte Besonderheiten und sicherheitsrelevante Vorgehensweisen ergänzt werden. SAP-eigene Sicherheitsvorkehrungen hinsichtlich Datenschutz und Datensicherheit werden nicht vergessen; das Audit Information System (AIS) für regelmäßige Sicherheitsüberprüfungen wird beschrieben. M 4.259 gibt wichtige Hinweise für den sicheren Einsatz der Benutzerverwaltung und für die den sicheren Umgang mit kritischen Berechtigungen.
Am Beispiel von SAP-Systemen werden deren besonderen Gefährdungen dargestellt, u.a.

- wesentliche größere Gefährdungen bei öffentlicher Netzanbindung,
- fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- unerlaubte Ausübung von Rechten,
- fehlende oder unzureichende Planung des SAP-Einsatzes,
- fehlerhafte Administration des IT-Systems und
- mangelnde Beteiligung von Mitarbeitern und Personalräten bei Outsourcing-Projekten.

Im Falle einer Einführung von SAP-Systemen werden u.a. Maßnahmen zur Schulung, Planung des SAP-Einsatzes, Planung von SAP-Berechtigungen, zum sicheren Betrieb von SAP-Systemen im Internet, zur Sicherheit beim Customizing von SAP-Systemen in Form von Checklisten beschrieben.
An den richtigen Schnittstellen werden auch Überwachungs- und Mitbestimmungsrechte der Personalräte angemessen berücksichtigt.

4. Zusammenführung von Datenschutz und Datensicherheit: Baustein 1.5 Datenschutz

Von großer Bedeutung für Personalräte ist der neue Baustein 1.5 Datenschutz in den IT-Grundschutz-Katalogen, der von den Datenschutzbeauftragten, der von den Datenschutzbeauftragten des Bundes und der Länder und den Aufsichtsbehörden der Länder für den nichtöffentlichen Bereich erarbeitet und verabschiedet wurde (Stand Juli 2007).[16] Der Datenschutzbaustein soll zukünftig in Zusammenarbeit mit dem BSI ständig fortentwickelt werden. Im Baustein 1.5 , der bereits auf große Nachfrage stößt, werden die Schnittstellen zwischen IT-Sicherheit und Datenschutz beschrieben, die Verantwortlichkeiten beim Datenschutz präzise erläutert, gesetzliche Vorgaben und konkrete Hilfestellungen zur Umsetzung des Datenschutz nach der IT-Grundschutz-Vorgehensweise gegeben und alle wichtigen auch für Personalräte aufgrund ihrer Überwachungsaufgabe zu berücksichtigenden gesetzlichen Rahmenbedingungen, Gefährdungen und Maßnahmen zur Gewährleistung des informationellen Selbstbestimmungsrechtes auch der Beschäftigten in Dienststellen und Unternehmen dargestellt.[17]

---

[15] HCM bedeutet Human Capital Management oder das Management des Humankapitals
[16] Eine nur noch vom BSI redaktionell zu überarbeitender Vorabdruck findet sich beim Internetauftritt des Bundesdatenschutzbeauftragten unter http://www.bfdi.bund.de
[17] Der besondere Nutzen dieses Bausteins für die Arbeit der Personalräte soll in einem gesonderten Artikel dargestellt werden.

5. Personalräte als Zielgruppe, Anwender und Nutznießer des IT-Grundschutzes

Die Mitbestimmung des Personalrates bei der Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, wird in den IT-Grundschutz-Katalogen eingearbeitet.
IT-Systeme, die sich prinzipiell zu Leistungs- und Verhaltenskontrollen eignen, unterliegen der Mitbestimmung des Personalrates gemäß § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz (BPersVG). Diese Vorschrift ist textidentisch zum § 87 Abs. 1 Nr. 6 BetrVG. Das Bundesverwaltungsgericht hat sich weitgehend an den Urteilen des Bundesarbeitsgerichts in Erfurt zu § 87 Abs. 1 Nr. 6 BetrVG angeschlossen.
Die Mitbestimmung bei Datensicherheitsmaßnahmen wie z. B. Protokollierung wird explizit angeführt. Die dabei erhobenen personenbezogenen Daten unterliegen einer strikten Zweckbindung, wie auch in Baustein 1.5 Datenschutz ausgeführt. Der Abschluss von einschlägigen Dienstvereinbarungen zu IT-Systemen wie z.B. SAP ist möglich. Bei konkreten Sicherheitsvorfällen wird auf die unbedingte Hinzuziehung des Personalrates hingewiesen, da ansonsten dienst- und arbeitsrechtliche Folgemaßnahmen hinfällig werden.
Ganz dringlich wird die frühzeitige Information und Kooperation mit dem Personalrat bei Projekten zum Outsourcing von Datenverarbeitung gesehen.
Werden Mitarbeiterdaten aus Datensicherungsgründen erhoben und verarbeitet, ist auch die Überwachungsaufgabe des Personalrates gemäß § 68 Abs. 1 Nr. 2 BPersVG zu beachten. Der Personalrat hat über die Einhaltung aller zugunsten der Beschäftigten geltenden Gesetze zu überwachen. Hierzu gehört auch das Bundesdatenschutzgesetz und insbesondere der § 9 und die dazugehörige Anlage. Entsprechende Paragrafen finden sich in allen Länderdatenschutzgesetzen.
Der § 9 ist die zentrale Datensicherheitsvorschrift und gilt immer dann, wenn das Bundesdatenschutzgesetz (BDSG) zur Anwendung kommt. Sie wendet sich an öffentliche Stellen des Bundes und nicht-öffentliche Stellen und Personen (Privatwirtschaft) gleichermaßen. Sie verlangt die Feststellung der Notwendigkeit von Schutzmaßnahmen im Rahmen einer standardisierten Risikoanalyse vor dem Einsatz der IT-Systeme. Für die Risikoanalyse sollte auf einschlägige Standards wie der IT-Grundschutz-Kataloge des BSI zurückgegriffen werden[18].
Personalräte auch als Anwender von Informationstechnik sollten ebenfalls diese Vorschrift beachten. Sie müssen für die Verarbeitung von personenbezogenen Daten im Personalratsbüro eigene Sicherheitsstandards definieren und umsetzen.

Fazit

Bei vielen wichtigen Aufgaben der Personalräte helfen die IT-Grundschutz-Kataloge. Von daher können Personalräte nur gewinnen, wenn sie in ihrer alltäglichen Mitbestimmungsarbeit auf die Vorarbeiten des Bundesamtes für Informationstechnik zurückgreifen. Mit der Integration des Datenschutzes in die IT-Grundschutz-Kataloge ist ein wichtiger Schritt zu mehr Datensicherheit und Datenschutz gelungen. Wir hoffen auf eine extensive Nutzung und Diskussion gerade auch bei Personalräten.

Dr. Eberhard Kiesche AoB Bremen
Matthias Wilke dtb Kassel

veröffentlicht in: der Personalrat 11/2007, 455ff

[18] Vgl. Wedde, a.a.O., § 9 BDSG, RdNr. 24