UIMC® - Pflichtenheft für die Sicherheit von IT-Systemen

Zielsetzung von IT-Sicherheitspflichtenheften

IT-Sicherheitspflichtenhefte haben die Zielsetzung, Normen, Maßstäbe und Sollvorstellungen festzulegen. Sie dienen in erster Linie dazu, bei

- Anschaffungsentscheidungen
- Umstrukturierungen oder
- Migrationsvorhaben

eine verläßliche Hilfe für die Beurteilung von Angeboten, Software-Lieferanten oder Kooperationspartnern, wie z. B. Outsourcing-Dienstleistern zu bieten. Darüber hinaus können IT-Sicherheitspflichtenhefte als Formulierung von Sollvorgaben auch dazu genutzt werden, betriebsintern als Richtschnur für Entwicklungsvorhaben zu dienen sowie die Tätigkeit der Mitarbeiter in einem bestimmten Projekt vorzustrukturieren und in der Ausführung zu kanalisieren. Hierdurch erweitert sich das o. a. Einsatzgebiet und macht ein so ausgelegtes Pflichtenheft zu einer wertvollen Arbeitsunterlage. Dies trifft in besonderem Maß für IT-Sicherheitspflichtenhefte zu, da bei den in diesen festgelegten Anforderungen sowohl die Auswahl- und Beurteilungs-komponente als auch der Anleitungscharakter für interne Projekte stark ausgeprägt ist und dementsprechend genutzt werden kann. IT-Leitungen werden häufig mit der Einführung von Anwendungen der Informationsverarbeitung (IT-Anwendungen) auf Datenverarbeitungsanlagen (z. B. SAP R3) konfrontiert.

Pflichtenheft für die Sicherheit von IT-Systemen

Pflichtenheftinhalte

- Grundlagen von Informationssystemen
- Anwendungsebene
- Betriebssytemebene
- Datenbankebene
- Netzwerkebene
- Organisation
- Buchhaltungsproblemstellungen
- Personalinformationssystem-besonderheiten
- Online-Services
- Protokollierungen
- Datenschutzbesonderheiten

Es ist oft nicht leicht zu erkennen, welche Auswirkungen sich hieraus auf die Sicherheitsproblematiken ergeben und welche Gestaltungsmöglichkeiten eine Standardsoftware bietet. Die Gestaltungsaufgaben beschränken sich dabei nicht alleine auf die Ergonomie. Vielmehr zielt eine Technikgestaltung auf eine ganzheitliche Betrachtung von Arbeit und Organisation. Zur Erleichterung der Arbeit bietet ein Pflichtenheft Handlungsgrundlagen, deren Beachtung davor schützt, Fehler bei Auswahl und Installation zu machen. Es werden Zielsetzungen, Gestaltungsmöglichkeiten und -ziele erläutert. Die Mitarbeiter sollen damit bei der Zielfindung und der Aufstellung eines Forderungskatalogs für konkrete Anwendungen unterstützt werden. Auch der Erstellung einer IV-Anwendung geht in der Regel die Formulierung eines IT-Sicherheitspflichtenheftes voraus. Darin wird festgelegt, welche Aufgaben mit dem System gelöst werden sollen, welche Eigenschaften das Programm haben soll und welche Anforderungen an Datenschutz und Datensicherheit gestellt werden. Derartige IT-Sicherheits pflichtenhefte dienen auch der Überwachung bestehender IT-Anwendungen. Kernelement ist ein umfassender Fragenkatalog, der es ermöglicht, IT-Systeme fachkundig auf ihre Sicherheitswirkung zu prüfen.

Einsatz von IT-Sicherheitspflichtenheften

Der Einsatz von IT-Sicherheitspflichtenheften hat üblicherweise zur Voraussetzung, dass eine verabschiedete Sicherheitszielsetzung vorliegt. Falls dies nicht der Fall sein sollte, können IT-Sicherheitspflichtenhefte eine solche unter bestimmten Bedingungen ersetzen oder ihre Erarbeitung unterstützen.
Falls eine Sicherheitszielsetzung vorhanden ist, ist das festgelegte Sicherheitszielniveau als Grundlage für die Wertungen des IT-Sicherheitspflichtenhefts zu übernehmen. Dies erleichtert die Arbeit mit dem IT-Sicherheitspflichtenheft. Bei Nichtvorhandensein eines Sicherheitszielniveaus ist es notwendig, die einzelnen Punkte jeweils im Hinblick auf die spezifischen Notwendigkeiten abzuprüfen. Hierbei wird folgendes Vorgehen empfohlen:

1. Bildung einer Arbeitsgruppe mit allen Beteiligten, die ein Mitspracherecht bei Sicherheitsfragestellungen haben. "Zwangsmitglieder" sind:
   - der Sicherheitsbeauftragte
   - der Datenschutzbeauftragte
   - Systemadministratoren
   - Benutzerservice
   - dezentrale IT-Koordinatoren
2. Diskussion und Verabschiedung der Bewertungsstufen. Unsere IT-Sicherheitspflichtenhefte schlagen ein bewährtes dreistufiges Bewertungssystem vor, vier- bis fünfstufige können genommen werden. Die Empfehlung lautet jedoch, ein dreistufiges Bewertungssystem zu verwenden.
3. Diskussion der einzelnen Positionen des IT-Sicherheitspflichtenhefts mit dem Ziel, für die einzelnen Merkmale Anspruchsniveaus festzulegen. Hierbei gilt, dass die Wertung "unbedingt notwendig" als K.o.-Kriterium wirkt: Falls eine Anwendung oder zur Diskussion stehende Standard software diese Kriterien nicht in dem geforderten Niveau erfüllt, ist entweder eine Nachkorrektur des Anspruchsniveaus vorzunehmen oder die betreffende Software scheidet mangels Erfüllung des Anspruchsniveaus aus. Die Reduzierung des Anspruchsniveaus ist jedoch bedenklich, da hiermit ein angestrebtes und für notwendig gehaltenes Sicherheitsniveau reduziert wird.
4. Es ist ein Protokoll zu erstellen, welches
   - Die verabschiedeten Sicherheitsansprüche ausweist,
   - diejenigen Merkmale festhält, bei denen das Sicherheitsanspruchsniveau nicht erfüllt werden konnte und
   - diejenigen Merkmale gesondert ausweist, bei denen ein ursprünglich festgelegtes Sicherheitsanspruchsniveau reduziert wurde, um Problemen zu begegnen. Insbesondere hierin liegen potentielle Sicherheitsschwachstellen des Systems.
5. Das IT-Sicherheitspflichtenheft ist dann dem Softwareerstellungs- oder Auswahlprozess zugrunde zu legen.
6. Besondere Bedeutung hat das IT-Sicherheitspflichtenheft im Customizing-Prozess. Von der Voraussetzung ausgehend, dass bei Standardsoftware die Auswahl anhand vorgegebener Kriterien vorgenommen wurde, ist im Customizing-Prozess die Realisierung vorzunehmen. Die Erfahrungen zeigen, dass aus Bequemlichkeit häufig beim Customizing-Prozess z. B. Default-Einstellungen nicht verändert werden, so dass für einen des Systems Kundigen "Sicherheitsscheunentore" geöffnet bleiben.
7. Ein nachgeschalteter Auditierungsprozess dient dazu, die Einhaltung der vorgegebenen Sicherheitskriterien der Art und Höhe nach sicherzustellen. Dieser kann eine Berichtigung des Zielniveaus erbringen, wird aber im Regelfall Handlungsanweisung für Korrekturen sein. Eine Auditierung kann über die Inhalte des Pflichtenhefts hinausgehen.

UIMC® **Dr. Vossbein GmbH & Co KG, Nützenberger Str. 119, 42115 Wuppertal**
Tel.: 0202-2 65 74 0, Fax: 0202-2 65 74 19, Internet: www.uimc.de, E-Mail: consultants@uimc.de