Die BSI-Grundschutz-Kataloge

Eberhard Kiesche // Matthias Wilke

Weitgehend unbeachtet von der Öffentlichkeit informierte das Bundesministerium des Inneren in einer Pressemeldung darüber, dass das Bundeskabinett am 5. September 2007 eine Erhöhung der Sicherheit auf Deutschlands Computern beschlossen hat. Im Windschatten der umstrittenen Onlinedurchsuchungen der PCs von Terrorverdächtigen ist ein „Nationaler Plan zum Schutz der Informationsinfrastrukturen" verabschiedet worden …

Die Bundesregierung reagierte mit diesem „Nationalen Plan zum Schutz der Informationsinfrastrukturen" (NPSI) auf die von ihr gesehene zunehmende Gefährdung der Informations- und Kommunikationstechnik (IKT). Steigende Zahlen von Computerviren, Phishing- und Hacker-Angriffen sowie die Zunahme der Wirtschaftsspionage (siehe J.-K. Klein: „Trau, schau, wem – wer spioniert denn wo?" in CuA 12/07) deuten die Bandbreite des Gefahrenpotenzials an. Immer öfter nutzen kriminelle Banden (ähnlich wie die „herkömmliche" organisierte Kriminalität) ▶ Viren, Würmer oder Trojanische Pferde, um an vertrauliche Daten zu kommen.

Der neue NPSI soll nun die verbindliche Sicherheitsleitlinie für den Schutz der sogenannten Informationsinfrastrukturen in allen Behörden des Bundes sein. Ebenso sollte er aber als Mindeststandard für die IKT-Sicherheit in der Privatwirtschaft gelten.

Das Bundesamt für Informationstechnik (BSI) wird die Umsetzung des Nationalen Plans koordinieren. Das BSI beschäftigt sich seit 1991 mit der IKT-Sicherheit und hat dazu seit 1995 mit ihrem „Grundschutz" bereits einen Quasi-Standard durchgesetzt. Aus dem damaligen IT-Grundschutzhandbuch sind mittlerweile die zusammen über 3600 Seiten starken IT-Grundschutz-Kataloge geworden. Dort gibt es – durchaus auch für Betriebs- und Personalräte – eine Fülle von Informationen, Methoden, Checklisten und Anleitungen zum Thema IKT-Sicherheit.

Die zentrale Idee der BSI-Grundschutz-Kataloge ist es, die IKT-Sicherheit kontinuierlich zu verbessern und schrittweise ein funktionierendes IKT-Sicherheitsmanagement in Unternehmen und Verwaltungen aufzubauen. In den im World-Wide-Web verfügbaren und praxistauglichen Katalogen findet sich dazu eine konkrete Anleitung.

Was hat nun der Betriebs- oder Personalrat damit zu tun? Jede Belegschaftsvertretung hat die Einhaltung aller zugunsten der Beschäftigten geltenden Gesetze und Vorschriften zu überwachen. Hierzu gehören natürlich auch entsprechende Normen und Standards. Und da IKT-Systeme in der Regel der Mitbestimmung durch den Betriebs- oder Personalrat unterliegen (nach § 87 Abs. 1 Nr. 6 BetrVG oder § 75 Abs. 3 Nr. 17 BPersVG) wird eine frühzeitige Information und Kooperation für alle Projekten der Datenverarbeitung auch vom BSI dringend empfohlen. Ausdrücklich wird auch darauf hingewiesen, dass bei konkreten Sicherheitsvorfällen die Belegschaftsvertretung unbedingt hinzugezogen werden muss.

Betriebs- und Personalräte, oder doch die entsprechenden Ausschüsse, tun deshalb gut daran, die Regeln und Normen der IT-Grundschutz-Kataloge zu kennen und zu beachten. Für die Mitgestaltung technischer Kontrolleinrichtungen und für die Organisation eines funktionierenden Datenschutzmanagements finden Belegschaftsvertretungen dort unentbehrliche Hinweise.

SEMINAR ZUM THEMA

Die IT-Grundschutz-Kataloge sind auch Thema eines Seminars (8.4.–10.4.2008 in Kassel) mit Schwerpunkt auf den daraus folgenden Handlungsmöglichkeiten für Betriebs- und Personalräte. Referenten: Dr. Peter Wedde, Professor für Arbeitsrecht und Recht der Informationsgesellschaft, und Ulrich Wiebel, Innenministerium NRW, Lizenzierter IT-Grundschutz-Auditor (BSI).

info@dtb-kassel.de, fon 0561 7057570

Autoren

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen, eberhard.kiesche@t-online.de;
Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel, info@dtb-kassel.de

Internet

Der Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI) sowie der Umsetzungsplan sind herunterzuladen unter www.bmi.bund.de

Informationen des BSI sind zu finden unter www.bsi.bund.de

Lexikon

Trojanische Pferde ▶ scheinbar nützliche Programme, die unbemerkt z.B. Datenbestände ausspionieren; fälschlich oft auch abgekürzt als „Trojaner" bezeichnet (tatsächlich richtete sich das „Trojanische Pferd" ja *gegen* die Trojaner)

Virus/Viren ▶ ein sich selbst vermehrendes kleines Programm, das sich meist via E-Mail oder Internet in ein IKT-System einschleust und dort nicht kontrollierbare Veränderungen vor allem am Betriebssystem oder an anderer Software vornimmt; oft auch als Sammelbegriff für alle Arten von Schadsoftware benutzt

Würmer ▶ auf Netzwerke spezialisierte Schadprogramme mit ähnlicher Wirkung aber anderer Technik als sie für Viren genutzt wird