DuD
Datenschutz und Datensicherheit

IT-Grundschutz

Stefan Gora, Claus Stark

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Das *IT-Grundschutzhandbuch* des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eine Empfehlung für informationstechnische Standard-Schutzmaßnahmen, die erstmals 1994 veröffentlicht und seitdem kontinuierlich weiterentwickelt und ergänzt wurden. Es besteht aus Bausteinen für viele IT-Infrastrukturkomponenten wie z. B. Firewalls und IT-Räume, die typische Gefährdungen beschreiben und Abwehrmaßnahmen empfehlen. In Deutschland hat es sich in vielen Unternehmen und Behörden als ein pragmatischer Ansatz für die Absicherung der Informations- und Kommunikationstechnik etabliert. Oft lässt sich bereits durch die im Grundschutzhandbuch beschriebenen Standard-Schutzmaßnahmen ein ausreichendes Maß an IT-Sicherheit erreichen. Aber auch bei weitergehenden Sicherheitsanforderungen leisten sie eine gute Basissicherung, auf denen spezielle Sicherheitsmaßnahmen aufsetzen können. Welche Bedeutung dem IT-Grundschutz beigemessen wird, zeigt der Beschluss der Bundesregierung zur „Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung" vom 16.01.2002: Ziel ist danach u. a. die flächendeckende Umsetzung von IT-Grundschutz für die elektronische Kommunikation an allen Arbeitsplätzen der Bundesverwaltung. Für die praktische Umsetzung von IT-Grundschutz in einem IT-Verbund (der genau definiert und abgegrenzt werden muss) schlägt das BSI mit dem IT-Grundschutzhandbuch folgende systematische Vorgehensweise vor:

Am Anfang jeder Grundschutz-Umsetzung steht eine *IT-Strukturanalyse*, die sich typischerweise am Netzplan des abzusichernden IT-Verbunds orientiert. Ein IT-Verbund kann eine Fachaufgabe (z. B. Bürokommunikation), ein Geschäftsprozess (z. B. Online-Banking) oder eine Organisationseinheit (z. B. eine Niederlassung) sein. Jede IT-Komponente ist eindeutig zu bezeichnen und kurz in Funktion und Eigenschaften zu beschreiben. Gleichartige Komponenten werden in Gruppen zusammengefasst. Aus dem so bereinigten Netzplan sind die IT-Systeme sowie die wichtigsten IT-Anwendungen (inklusive der mit ihnen verarbeiteten Daten) zu erheben.

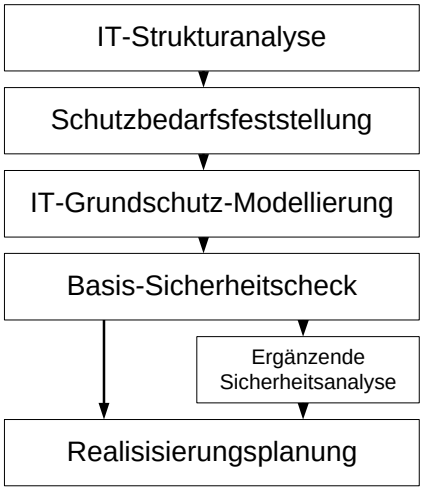

Abbildung: Erstellung des Sicherheitskonzepts nach IT-Grundschutz

In der *Schutzbedarfsfeststellung* werden die kritischen Anwendungen des IT-Verbunds identifiziert (Schutzbedarf „niedrig/mittel" für Anwendungen, deren Schadensauswirkungen sehr begrenzt sind bis hin zu Schutzbedarf „hoch" oder „sehr hoch" bei möglichen beträchtlichen bzw. katastrophalen Auswirkungen). Anwendungen, für die ein höherer Schutzbedarf festgestellt wird (z. B. die personenbezogenen Daten der Personaldaten-DV) sind besser abzusichern als solche mit niedrigem Schutzbedarf (z. B. das Textverarbeitungssystem für die Erstellung des Kantinenplans). Diese Bewertung ist sehr individuell, denn oft können Schäden, die für das eine Unternehmen vernachlässigbar erscheinen, ein anderes Unternehmen existentiell bedrohen. Aus dieser Bewertung leitet sich der Schutzbedarf der IT-Systeme, Kommunikationsverbindungen und IT-Räume ab. Es ist darauf zu achten, dass die gewählten Schutzbedarfskategorien in sich konsistent, plausibel und vollständig sind.

Mit der *Modellierung nach IT-Grundschutz* werden die notwendigen Sicherheitsmaßnahmen zum Schutz des IT-Verbunds ermittelt. Das Grundschutzhandbuch gliedert konkrete Maßnahmen in Bausteinen, die selbst wieder jeweils einer von fünf Schichten (Übergeordnete Aspekte, Infrastruktur, IT-Systeme, Netze und IT-Anwendungen) zugeordnet sind. Jeder Baustein beschreibt für ein bestimmtes Thema (z. B. IT-Sicherheitsmanagement, Büroraum oder Windows 2000-Client) die typischen Gefährdungen und hierzu geeigneten Sicherheitsmaßnahmen. Alle für den IT-Verbund relevanten Bausteine sind bei der Modellierung anzuwenden.

Im *Basis-Sicherheitscheck* schließlich wird der aktuelle Umsetzungsgrad der Sicherheitsmaßnahmen erhoben. Diese Erhebung erfolgt u. a. durch Befragung der zuständigen Verantwortlichen. Im anschließenden Soll-Ist-Vergleich werden die Lücken identifiziert (die es zu beseitigen gilt).

Wurden im Rahmen der Schutzbedarfsfeststellung ein hoher oder sehr hoher Schutzbedarf festgestellt, sind *ergänzende Sicherheitsanalysen* durchzuführen (z. B. Netzwerk-Penetrationstests) und ggf. spezielle Schutzmaßnahmen (die über die Standard-Schutzmaßnahmen hinausgehen können) zu ergreifen.

Bei der *Realisierung der IT-Sicherheitsmaßnahmen* schließlich sind die konsolidierten und priorisierten Sicherheitsmaßnahmen praktisch umzusetzen.

Das im Februar 2002 veröffentlichte *Qualifizierungs- und Zertifizierungsschema für IT-Grundschutz* des BSI gibt Behörden und Unternehmen nun die Möglichkeit, die wirkungsvolle Umsetzung von IT-Grundschutzmaßnahmen mit einem unabhängigen *Audit* durch lizenzierte IT-Grundschutz-Auditoren und der Erteilung eines *IT-Grundschutz-Zertifikats* gegenüber den Mitarbeitern, Geschäftspartnern, Kunden und Behörden zu dokumentieren (siehe Münch, DuD 6/2002, S. 346 ff).