Beauftragter für IT Sicherheit

Dipl.-Inf. (Univ) Rudolf Zenkert

Jeder Betreiber und Benutzer von IT-Systemen und Rechnernetzen hat auf Grund seiner Sorgfaltspflicht Belange der IT-Sicherheit in ausreichendem Maße zu berücksichtigen. So wird von den Rechnungshöfen des Bundes und der Länder in einer Studie zu IuK-Mindestanforderungen (Bund, 26.9.2001) explizit auf die Sicherheit beim Einsatz von IuK eingegangen. Die Aufgaben des Beauftragten für IT-Sicherheit sind also nicht neu hinzugekommen, sondern waren schon immer ein Bestandteil der Arbeit im Bereich der IT. Durch die weitere Durchdringung der IT in den Behörden und neue Bedrohungsszenarien ist dem Bereich IT-Sicherheit mehr Bedeutung zu schenken.

1. Auftrag

Alle Behörden, die einen Zugang zum Bayerischen Behördennetz betreiben, sind verpflichtet, einen Beauftragten für IT-Sicherheit aus ihrem eigenen Bereich benennen. Für eine ausreichende Stellvertretung ist jeweils Sorge zu tragen. Der Beauftragte für IT-Sicherheit dient als Ansprechpartner für IT-sicherheitsrelevante Themen im eigenen Zuständigkeitsbereich. Die Aufgaben des Beauftragten für IT-Sicherheit sind analog zum Datenschutzbeauftragten in erster Linie beratend und koordinierend und weniger im operativen Bereich.

Der Beauftragte für IT-Sicherheit erfüllt zudem eine qualitätssichernde Funktion für IT-Sicherheit, indem er die Wirksamkeit der technischen und organisatorischen Maßnahmen überprüft oder überprüfen lässt. Wegen der grundsätzlichen Konkurrenzsituation zwischen technischem Betrieb und Sicherheit sollte der Beauftragte nach Möglichkeit nicht direkt in den Betrieb der IT-Infrastruktur eingebunden sein.

Die grundsätzlichen Aufgaben ergeben sich direkt aus der IT-Sicherheitsleitlinie [1] und der Richtlinie zur IT-Sicherheitsorganisation der bayerischen Staatsverwaltung [2](s. Abb. 1).

1.1 Ansprechpartner für alle IT-sicherheitsrelevanten Themen

Der Beauftragte für IT-Sicherheit soll als koordinierender und fokussierender Ansprechpartner im Bereich des LfStaD fungieren und die Schnittstelle zwischen

- den Servicegruppen der einzelnen Betriebsbereiche,
- dem Bayern-CERT,
- dem Sicherheitsteam des bayerischen Behördennetzes
- und den Kunden des künftigen RZ-Süd mit ihren verfahrensspezifischen Anforderungen im Bereich der IT-Sicherheit bilden.

Er soll bei allen IT-sicherheitsrelevanten Themen und Projekten einbezogen und informiert werden. Dies umfasst die Unterstützung

Abb. 1

bei der Erstellung und Realisierung von Sicherheitskonzepten für die einzelnen Fachverfahren sowie die Beratung und Betreuung von IT-Nutzern.

Gemäß der Geschäftsordnung für das Sicherheitsteam des bayerischen Behördennetzes [3] entsendet auch das LfStaD neben dem CERT ein Mitglied mit beratender Stimme in das Gremium. Der Beauftragte für IT-Sicherheit hat damit die Aufgabe, die Belange des LfStaD im Sicherheitsteam in geeigneter Weise zu vertreten.

1.2 Aufbau einer geeigneten Sicherheitsorganisation

Als weitere wichtige Aufgabe ist der Aufbau einer Sicherheitsorganisation zu nennen, die den Beauftragten unterstützt und für die korrekte und zeitnahe Ausführung der erforderlichen Maßnahmen Sorge trägt.

„Die Verantwortung für den sicheren Umgang mit Daten, Systemen und Netzwerkkomponenten ist festzulegen. Für jeden Verantwortlichen ist ein Vertreter zu benennen. Änderungen in der Verantwortung sind schriftlich festzuhalten und der zuständige Beauftragte für IT-Sicherheit ist unverzüglich zu informieren" [1].

Ein angemessenes Sicherheitsniveau kann nur durch geplantes und zielgerichtetes Vorgehen aller Beteiligten durchgesetzt und aufrechterhalten werden. Voraussetzung hierfür ist die Wahrnehmung der Planungs- und Lenkungsaufgabe durch ein IT-Sicherheitsmanagement(-Team), das in die existierenden Organisationsstrukturen des LfStaD eingebettet ist.

Im Einzelnen sind die Rollen, Zuständigkeiten und Schnittstellen bei der Abhandlung von IT-Sicherheitsvorfällen (z.B. Virenbefall) und bei der Erstellung von IT-Sicherheitskonzepten festzulegen. Idealerweise orientieren sich die Rollen an den Zuständigkeiten der einzelnen Servicegruppen (Administration der Plattformen, zentrale Dienste des Behördennetzes etc.) im LfStaD.

Für die Eskalation von Sicherheitsvorfällen sind entsprechende Meldewege und Prozesse festzulegen (s. Abb. 2).

1.3 Mitwirkung bei der Erstellung von Sicherheitskonzepten

Die konkrete Umsetzung der IT-Sicherheitsleitlinie und der IT-Sicherheitsrichtlinien erfolgt im Rahmen von Sicherheitskonzepten und der Definition von Sicherheitsregeln für kritische oder sensible Geschäftsprozesse.

Sicherheitskonzepte und Sicherheitsregeln für einzelne Geschäftsprozesse sind bereichsspezifisch, also unter der Federführung des Beauftragten für IT-Sicherheit der jeweiligen Behörde, zu erstellen und umzusetzen. Er erstellt hierzu ein Sicherheitsrahmenkonzept für die gesamte IT in der Behörde (einschl. angebotener Dienstleistungen für Dritte) und konkretisiert den Schutzbedarf und die zu ergreifenden Sicherheitsmaßnahmen einzelner Fachverfahren und Dienste im Behördennetz durch detaillierte Sicherheitskonzepte.

Grundsätzlich ist der Beauftragte für IT-Sicherheit dafür verantwortlich, dass beim Erstellen eines konkreten Sicherheitskonzepts die übergeordneten Richtlinien angewandt und eingehalten werden.

1.4 Koordination der Umsetzung erforderlicher Maßnahmen zur IT-Sicherheit

Für die Erstellung der Sicherheitskonzepte ist die aktive Mitwirkung der betroffenen Fach- und Betriebsgruppen (z.B. Betreiber eines Verfahrens) erforderlich, der Beauftragte für IT-Sicherheit koordiniert die erforderlichen Maßnahmen und dient als fachlicher und organisatorischer Ansprechpartner für die beteiligen Mitarbeiter. Er muss dabei die erforderlichen technischen und organisatorischen Implementierungen durch den Betrieb veranlassen, eine aussagekräftige Dokumentation einfordern und die Einhaltung und Wirksamkeit der Maßnahmen regelmäßig überprüfen. Darüber hinaus ist er für die Schulung und Sensibilisierung der Nutzer und Administratoren verantwortlich.

2 Situation im LfStaD

Die Funktion des Beauftragten für IT-Sicherheit wurde zum 01.10.2004 im LfStaD eingerichtet und orientiert sich an den im vorangegangenen Abschnitt dargelegten Aufgaben.

Unter Berücksichtigung der bisherigen Entwicklung in den IT-Bereichen im LfStaD ergeben sich daraus folgende vordringliche Aufgaben:

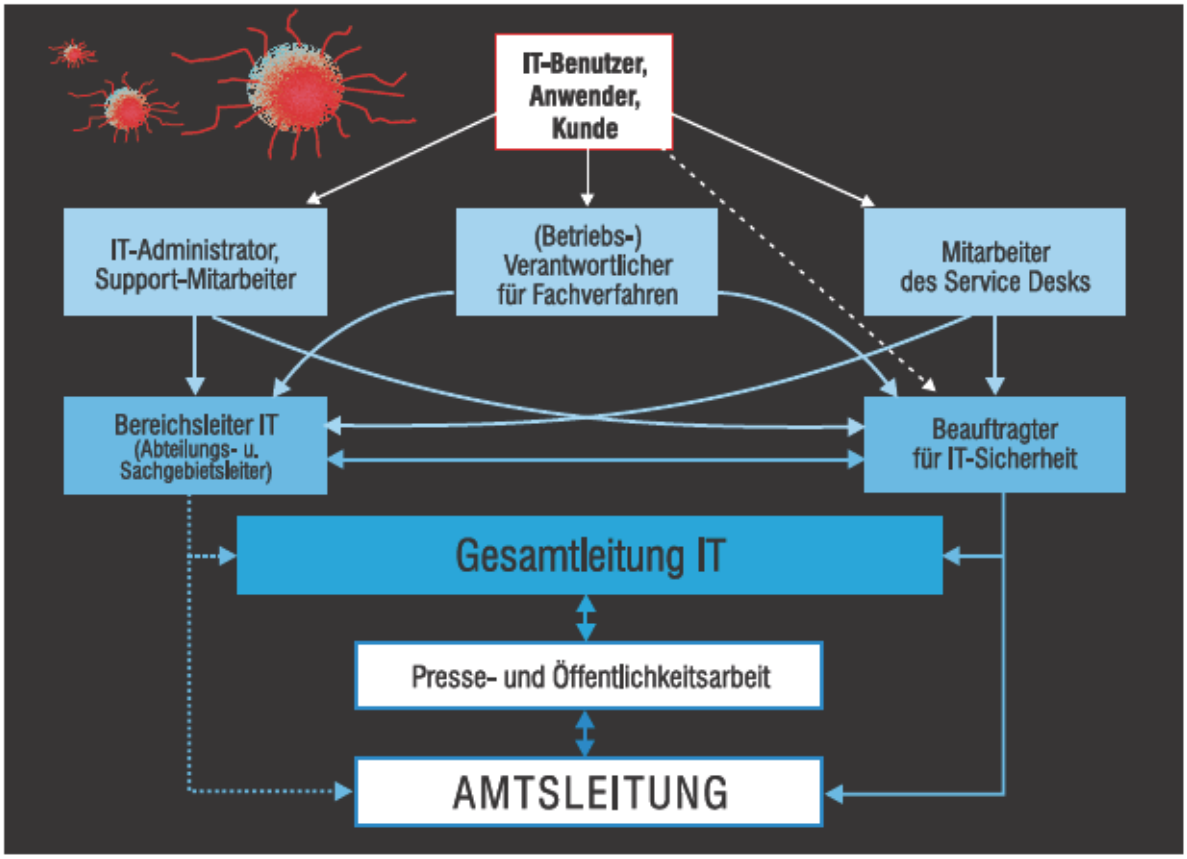
a) Definition und Etablierung eines IT-Sicherheitsprozesses im LfStaD
b) Erstellung eines Sicherheitsrahmenkonzepts, in dem die grundlegenden Rahmenbedingungen der IT-Sicherheit identifiziert und die erforderlichen allgemeinen Vorgaben beschrieben werden
c) Erstellung, Vervollständigung und zeitnahe Aktualisierung von IT-Sicherheitskonzepten für alle IT-Bereiche und IT-Komponenten im LfStaD

2.1 Einrichtung eines IT-Sicherheitsprozesses im LfStaD

Der Beauftragte für IT-Sicherheit kann seine Aufgaben nur dann effizient und sachgerecht erfüllen, wenn bestimmte organisatorische Anforderungen erfüllt sind:

a) Durch die Behördenleitung muss ein gesteuerter IT- Sicherheits-

Abb. 2



prozess initiiert werden, der die Voraussetzungen für die durchdachte Gestaltung, die sinnvolle Umsetzung von IT-Sicherheitsmaßnahmen sowie eine Erfolgskontrolle gewährleistet.

b) Die Planungs- und Lenkungsaufgaben müssen durch ein IT-Sicherheitsmanagement(-Team) wahrgenommen werden, das entsprechende Unterstützung durch die Leitungsebene / Amtsleitung erfährt.

Folgende Funktionen werden typischerweise durch das IT-Sicherheitsmanagement wahrgenommen:

- Festlegung persönlicher Verantwortungsbereiche
- Vorgabe/Abstimmung strategischer und konzeptioneller Ziele
- Ressourcenrelevante Entscheidungen (Personal, Sachmittel)
- Überörtliche Abstimmung (soweit erforderlich)
- Unterstützung der Projektverantwortlichen bei der Durchsetzung von Sicherheitsmaßnahmen

c) Aufgaben und Zuständigkeiten müssen definiert und der Funktion „Beauftragter für IT-Sicherheit" zugeordnet werden. Die Funktion muss in den einzelnen Organisationsbereichen des LfStaD hinlänglich bekannt sein und von ihnen aktiv unterstützt werden.

d) Der Betrieb des LfStaD (einschl. Projektsteuerung, Entwicklung) umfasst eine Vielzahl von Prozessen und Abläufen. Der Beauftragte für IT-Sicherheit muss in diese Abläufe eingebunden werden, damit die Belange der Sicherheit entsprechend berücksichtigt werden können.

Konkret betrifft es:

- (Beratungs-)Gespräche mit Kunden zur Übernahme von Fachverfahren in den Betrieb des Rechenzentrums
- Entwicklung von Verfahren zum späteren Betrieb im Rechenzentrum
- Ausbau und Aktualisierung von Komponenten der IT-Infrastruktur
- Etablierung von Prozessen aus dem Bereich IT-Service-Management (ITIL)
- Sachgerechte Eskalation von Sicherheitsvorfällen

Darüber hinaus muss ein entsprechender Informationsfluss (IT-Sicherheits-Know-How, betriebliche Fachkenntnisse) etabliert werden, von dem die Servicegruppen des LfStaD und der Beauftragte für IT-Sicherheit gleichermaßen profitieren.

2.2 Erstellung eines Rahmenkonzeptes für die gesamte IT-Sicherheit

Die flächendeckende, verfahrensgerechte Einführung von IT-Sicherheit erfordert ein planmäßiges und abgestimmtes Vorgehen, nicht zuletzt um die vorhandenen Ressourcen bestmöglich einsetzen zu können. Darüber hinaus sind grundsätzliche Entscheidungen und

Festlegungen zu treffen, die sich auf die künftige Realisierung der IT-Sicherheit beziehen:

- Generelles und koordiniertes Vorgehen zur Etablierung der IT-Sicherheit (Initiierung des IT-Sicherheitsprozesses)
- Definition von Rahmenbedingungen für detaillierte Sicherheitskonzepte zu einzelnen Verfahren und Komponenten
- Einführung von technischen und organisatorischen Sicherheitsmaßnahmen mit dem Ziel einer späteren Zertifizierung
- Verpflichtung zur Durchführung regelmäßiger Sicherheitsüberprüfungen (Security Audits)
- Öffentlichkeitswirksame Darstellung der Maßnahmen zur IT-Sicherheit
- Koordination von Audits kundenspezifischer Verfahren im Hinlick auf Maßnahmen zur IT-Sicherheit der zentralen Komponenten der IT-Infrastruktur

2.3 Erstellung und zeitnahe Aktualisierung von IT-Sicherheitskonzepten

Das LfStaD ist sowohl für die eigenen Organisationseinheiten (u.a. Statistik) als auch für alle anderen bayerischen Behörden zentraler IT-Dienstleister im Bereich des bayerischen Behördennetzes. Die Dienstleistungen umfassen eine Vielzahl fachspezifischer Verfahren und die Bereitstellung zentraler Komponenten für das bayerische Behördennetz (z.B. Firewall, Virenschleuse).

Zur Abschätzung des für die Erstellung von Sicherheitskonzepten und -regeln erforderlichen Aufwands ist eine qualitative und quantitative Aufnahme des derzeitigen Standes der IT-Sicherheit erforderlich. Es sind dabei alle sicherheitsrelevanten Abläufe, Verfahren und Komponenten zu berücksichtigen, ferner sind die für die einzelnen Verfahren und Komponenten verantwortlichen Mitarbeiter / Servicegruppen zu dokumentieren.

Mit der Beschreibung des Ist-Zustandes im Bereich der IT-Sicherheit können die weiteren erforderlichen Aktivitäten geplant werden:

a) Ermittlung des notwendigen Schutzbedarfes der einzelnen Verfahren und Komponenten anhand konkret existierender Bedrohungsszenarien
b) Bewertung des jeweiligen Sicherheitsrisikos und damit der Dringlichkeit für die einzelnen erforderlichen Konzepte
c) Zusammenfassung von Abläufen, Verfahren etc. in übergreifend zu erstellenden Sicherheitskonzepten
d) Abschätzung des Aufwandes für die Erstellung neuer bzw. Vervollständigung vorhandener Sicherheitskonzepte

IT-Sicherheit kann nur dann ihre Wirkung voll entfalten, wenn Sicherheitskonzepte und Sicherheitsregeln zeitnah in der Praxis umgesetzt werden. In vielen Fällen wird dies gelingen, da vom Betrieb bereits konkrete Sicherheitsmaßnahmen ergriffen wurden, die nur noch entsprechend ihrem aktuellen Stand dokumentiert werden müssen.

In allen anderen Fällen müssen die Sicherheitskonzepte und Sicherheitsregeln zusammen mit den für den Betrieb verantwortlichen Mitarbeitern diskutiert und erarbeitet werden. Sicherheitskritische Geschäftsprozesse sowie notwendige technische und organisatorische Maßnahmen sind entsprechend zu beschreiben. Dabei ist darauf zu achten, dass sich die Konzepte am technisch und organisatorisch Machbaren orientieren und zeitnah im täglichen Betrieb umgesetzt werden können.

2.4 Qualitätssicherung und Überprüfung der Sicherheitsmaßnahmen

Die zu den einzelnen Themen und Bereichen der IT-Sicherheit erstellten oder ergänzten Dokumente zur IT-Sicherheit sollten im Rahmen einer umfassenden Qualitätssicherung auf ihre Vollständigkeit und Schlüssigkeit sowie auf ihre technische Aktualität hin überprüft werden. Diese Prüfung kann schrittweise im Rahmen eines oder mehrerer Security Audits stattfinden. In der Folge ist es dann notwendig, die eingeleiteten Maßnahmen regelmäßig auf Ihre permanente Einhaltung und auf Ihre (technische) Aktualität hin zu überprüfen. Dabei fließen auch Erfahrungen aus dem praktischen Betrieb bzw. geänderte Anforderungen und Rahmenbedingungen ein.

3 Literatur

[1] Sicherheitsleitlinie für die bayerische Staatsverwaltung, http://www.bybn.de/RBIS/BYBN/MIG/sicherheitsleitlinie.pdf

[2] Richtlinie zur IT-Sicherheitsorganisation in der Bayerischen Staatsverwaltung http://www.bybn.de/RBIS/BYBN/MIG/organisationsrichtlinie.pdf

[3] Geschäftsordnung für das Sicherheitsteam der Bayerischen Staatsverwaltung http://www.bybn.de/RBIS/BYBN/MIG/go-sicherheitsteam.pdf