

Bonno Domke / Nils Dirks

Schutz für Zensusdaten

Im Rahmen der aktuellen Volkszählung werden sensible Personendaten auf elektronischem Wege an die zuständigen Ämter übermittelt. Das Statistische Landesamt Hessen hat seine IT-Infrastruktur daher im Vorfeld des Zensus 2011 einer umfassenden Sicherheitsanalyse unterzogen.

Ein funktionierender Staat braucht eine solide Planungsbasis. Diese wird in vielen Bereichen auch durch statistische Daten geschaffen. Jedoch sind nicht alle verfügbaren statistischen Daten aktuell. So basieren zum Beispiel die vorhandenen Bevölkerungs- und Wohnungszahlen auf statistischen Fortschreibungen der Volkszählung des Jahres 1987 der früheren BRD und der Volkszählung des Jahres 1981 der DDR. Der lange Zeitraum der Fortschreibung und die großen Veränderungen in der Zeit nach der Wiedervereinigung führen zwangsläufig zu Ungenauigkeiten; die Zahlen dienen jedoch weiterhin als Grundlage für wichtige politische und infrastrukturelle Entscheidungen. So haben die aktuellen amtlichen Einwohnerzahlen beispielsweise direkten Einfluss auf den vertikalen und horizontalen Finanzausgleich, die Einteilung der Bundestagswahlkreise oder die Sitze Deutschlands im Europaparlament.

Mit der Durchführung des Zensus 2011 werden die statistischen Fortschreibungen an die realen Umstände in Deutschland angepasst. Darüber hinaus werden Informationen zum Wohnraum, zur Bildung und zum Erwerbsleben erhoben, um auf dieser Basis beispielsweise die Haushalts- und Infrastruktur-

planung vornehmen zu können. Der Zensus 2011 ist ein gemeinsames Projekt der statistischen Ämter des Bundes und der Länder. Im Gegensatz zu früheren Volkszählungen bilden dabei Daten aus Verwaltungsregistern die Grundlage. Sie werden ergänzt um eine Stichprobe von zehn Prozent der Bevölkerung. Lediglich bei den Grundstücks- und Wohnungseigentümern erfolgt eine vollständige schriftliche Befragung. Bis zum Jahr 2013 werden dann viele Millionen Datensätze ausgewertet, um aktuelle Zahlen zum Leben, Wohnen und Arbeiten in Deutschland zu gewinnen.

Brisante Datensätze

Die Datensätze des Zensus sind von erheblicher Brisanz, da zum einen die den Statistikämtern übermittelten Rohdaten überwiegend sensibel und personenbezogen sind, und zum anderen die verarbeiteten Daten von hohem strategischen Wert für eine nachhaltige Steuerung der Entwicklung in Deutschland sind. Aus diesem Grund hat das Hessische Statistische Landesamt (HSL) im Vorfeld des Zensus 2011 eine Sicherheitsanalyse beauftragt. Der Fokus lag dabei auf der für den Zensus relevanten IT-Infrastruktur und den organisatorischen Prozessen in Hes-

sen. Die Sicherheitsanalyse wurde im Zeitraum von Juni bis Oktober 2010 von der Firma rt-solutions.de durchgeführt, bevor ab dem 1. November 2010 die ersten elektronischen Zensusdaten an das HSL übermittelt wurden. Im Rahmen der Analyse wurden Abweichungen von Best Practices innerhalb des Hessischen Statistischen Landesamtes identifiziert und gemäß den gesetzlichen Vorgaben angemessene bauliche, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbefugter Einsichtnahme, Missbrauch und Fälschung empfohlen.

Die Sicherheitsanalyse des Zensus 2011 für das HSL erfolgte nach der IT-Grundschutzmethode des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Standard 100-2). Diese bietet unter anderem eine Basis für die Überprüfung des vorhandenen IT-Sicherheitsniveaus sowie die Umsetzung einer angemessenen IT-Sicherheit und stützt sich dabei auf die im IT-Grundschutzkatalog enthaltenen Gefähr-

Kurz gefasst

Als Vorbereitung auf den Zensus 2011 wurden IT-Infrastruktur und organisatorische Prozesse im Hessischen Statistischen Landesamt auf mögliche Sicherheitslücken überprüft. Der Beitrag beschreibt Ablauf und Ergebnis der IT-Sicherheitsanalyse.

dungen und Schutzmaßnahmen für typische Informationswerte.

Für Informationswerte mit normalem Schutzbedarf ist es ausreichend, die dort genannten organisatorischen, personellen und technischen Standardmaßnahmen anzuwenden. Bei Schutzbedarfen, welche über diesen Grundschatz hinausgehen, sollte ergänzend eine zusätzliche Sicherheitsanalyse durchgeführt werden. Das Vorgehen im Rahmen der Sicherheitsanalyse für den Zensus 2011 gliederte sich gemäß BSI-Grundschatz in die Phasen IT-Strukturanalyse, Schutzbedarfsfeststellung und Sicherheitskonzeption.

IT-Verbund dokumentieren

Ziel der IT-Strukturanalyse war es, den IT-Verbund – den Gegenstand des Sicherheitskonzeptes – abzugrenzen und strukturiert zu beschreiben. Diese Beschreibung bildete die Grundlage für die anschließende Modellierung nach IT-Grundschatz und die Auswahl von Schutzmaßnahmen. Der IT-Verbund umfasste dabei alle infrastrukturellen, technischen und organisatorischen Komponenten, die mit dem Zensus 2011 innerhalb des HSL in Zusammenhang stehen. Für die IT-Strukturanalyse wurden die Daten vollständig erfasst und ausgewertet, basierend auf den Erhebungen der Datenbestände, des Netzplans, der Anwendungen, der IT-Systeme, der Personen und der Räume. Um die Menge der erfassten Daten zu reduzieren ohne einen Verlust von Informationen hinnehmen zu müssen, wurden die Daten in Gruppen zusammengefasst, die ähnliche Merkmale aufweisen. So wurden beispielsweise Server gleicher Art

oder Personen mit gleichen Tätigkeitsbereichen jeweils zu Gruppen zusammengefasst. Einzelne Komponenten einer Gruppe wurden dann bei der Modellierungsphase gemeinsam betrachtet. Die gesamte Dokumentation des IT-Verbunds wurde mithilfe des BSI-Grundschatz-Tools vorgenommen.

Die korrekte Modellierung nach IT-Grundschatz setzt eine SchutzbedarfsEinstufung für alle Informationswerte, also Datenbestände, Anwendungen, IT-Systeme und Räume, voraus. Die SchutzbedarfsEinstufung richtet sich primär nach dem maximal zu erwartenden Schaden, wenn eines der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit verletzt wird. Wirken mehrere Informationswerte mit dem einzustufenden

Wert zusammen – beispielsweise mehrere Anwendungen auf einem IT-System –, wird die schwerwiegendste Auswirkung auf dessen Schutzziele vererbt (Maximumprinzip). Die von IT-Grundschatz vorgegebenen Schutzbedarfskategorien umfassen:

- Normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
- Hoch: Die Schadensauswirkungen können beträchtlich sein.
- Sehr hoch: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Auf Basis der anwendbaren Prozesse des Zensus 2011 innerhalb des HSL wurden zunächst die Schutzbedarfe der zu verarbeitenden Daten pro Schutzziel festge-



Mit Haufe sind Sie beim Datenschutz auf der sicheren Seite. Versprochen.

Mit „Datenschutz-Management“ erledigen Sie als Datenschutz-Verantwortlicher alle anstehenden Aufgaben effizient und dokumentieren Ihre Tätigkeit systematisch.

NEU: inkl. Online-Seminaren zu aktuellen Top-Themen.

legt. Diese Schutzbedarfe wurden dann im zweiten Schritt an die Anwendungen vererbt. Diese vererbten wiederum ihre Schutzbedarfe an die IT-Systeme, auf denen sie laufen. Der Schutzbedarf der IT-Systeme bestimmte dann auch die Schutzbedarfe der Räumlichkeiten, in denen sie betrieben wurden. Abweichungen von diesem Prinzip durch Kumulations- oder Verteilungseffekte wurden formal begründet im Grundschutz-Tool festgehalten.

Maßnahmen empfehlen

Mit einem vollständigen Inventar der Informationswerte nebst Schutzbedarfeinstufung wurden anschließend die Bausteine des IT-Grundschutzkatalogs angewendet. Um dies für das Hessische Statistische Landesamt umfassend tun zu können, musste zunächst die Bedrohungslage für die Daten des Zensus 2011 analysiert werden. Durch die komplexe Struktur des Datenaustausches und der damit verbundenen hohen Anzahl an Schnittstellen zu anderen Landesämtern sowie dem Statistischen Bundesamt ist der IT-Verbund einer Reihe von unterschiedlichen Gefahren ausgesetzt, die im Detail betrachtet werden mussten. Auf Basis dieser Analyse und des existierenden generischen, bundesweiten Sicherheitskonzeptes für den gesamten Zensus 2011 wurden die wichtigsten Maßnahmen für die jeweils betroffenen Komponenten aus dem Grundschutzkatalog ausgewählt, gruppiert und priorisiert. So wird sichergestellt, dass die erforderlichen Schutzmaßnahmen zum Start des Zensus auf jeden Fall identifiziert und umgesetzt werden konnten.

Durch Prüfung der priorisierten Maßnahmenempfehlungen wurde abschließend ermittelt, ob und inwieweit die empfohlenen Maßnahmen im Hessischen Statistischen Landesamt bereits umgesetzt wurden und an welcher Stelle noch Handlungsbedarf bestand. Dies erfolgte in Form eines Soll-Ist-Vergleichs anhand der Maßnahmenempfehlungen für den Zensus 2011 und in enger Kooperation mit der IT-Leitung des HSL. Als entbehrlich galt eine Maßnahme beispielsweise, wenn ihre Umsetzung für einen betrachteten Einsatzzweck nicht relevant war. Die Anwendbarkeit einer Maßnahme war abhängig vom festgelegten Gültigkeitsbereich und der Identifizierung einer relevanten Schwachstelle.

In beiden Fällen wurde das Ergebnis der Maßnahmenempfehlung stichhaltig begründet und

schriftlich so festgehalten, dass es auch von Dritten nachvollzogen werden kann. Das Ergebnis entsprach einer Auflistung aller Schutzmaßnahmen, die bisher nur teilweise und/oder noch nicht realisiert wurden und bis zum Start des Zensus durch das HSL umgesetzt werden mussten.

Ziel: Zertifizierung

Mithilfe der Sicherheitsanalyse des Zensus 2011 in Hessen konnten Abweichungen vom BSI Standard 100-2 bezüglich der Aufrechterhaltung der Informationssicherheit identifiziert werden. Diese Abweichungen wurden anschließend den verantwortlichen Entscheidungsträgern vorgestellt und eine entsprechende Auswahl von priorisierten Maßnahmen zu deren Behebung empfohlen. Die jeweiligen Verantwortlichen sind sich somit der Schwachstellen in ihren Aufgabenbereichen bewusst und können diese gezielt angehen. Die Umsetzung von Maßnahmen hoher Priorität wurde zeitnah eingeleitet, die übrigen Abweichungen wurden bis Beginn des Zensus am 9. Mai 2011 behoben.

Die Sicherheitsanalyse sorgte beim Hessischen Statistischen Landesamt letztlich nicht nur für eine Verbesserung der Informationssicherheit, sondern hinterließ auch eine im Grundschutz-Tool gepflegte, aktuelle Dokumentation des IT-Verbundes des Zensus 2011. Diese dient als Quelle für weitere Sicherheitsanalysen. Darüber hinaus wurde im Rahmen der durchgeführten Sicherheitsanalyse die erste Etappe im Hinblick auf das langfristige Ziel einer BSI-Zertifizierung erreicht. ◀

Die Autoren: Bonno Domke und Nils Dirks



Bonno Domke ist seit 1998 Leiter der Abteilung „Informationstechnologien, Unternehmensregister, Gewerbeanzeigen“ im Hessischen Statistischen Landesamt. Nils Dirks ist als Diplom-Informatiker seit 2005 bei der rt-solutions.de GmbH tätig.