Nordrhein-Westfalen

Tipps für Kommunen

[17.11.2016] Um den Stand der IT-Sicherheit in nordrhein-westfälischen Kommunen im Kontext kritischer Infrastrukturen zu ermitteln, hat die Gemeindeprüfungsanstalt Nordrhein-Westfalen Prüfberichte ausgewertet und Empfehlungen herausgearbeitet.

Im Zuge überörtlicher Prüfungen bei den Gemeinden und Landkreisen untersucht die Gemeindeprüfungsanstalt Nordrhein-Westfalen (GPA NRW) den organisatorischen IT-Aufbau. Ein Teilaspekt ist die IT-Sicherheit. Auf diesen Aspekt hin hat die GPA im Arbeitskreis Kritische Infrastrukturen 32 bereits veröffentlichte Prüfberichte ausgewertet. Dazu wurden Schlagwörter aus den Berichten mithilfe einer quantitativen Inhaltsanalyse extrahiert, gezählt und in zwei Ranglisten dargestellt. Eine Rangliste enthält positive Bewertungen mit fortführenden Empfehlungen, die andere negative Bewertungen und unzureichende Sicherheitsvorkehrungen, die Handlungsbedarf erfordern. Synonyme und ähnliche Formulierungen wurden thematisch zusammengefasst. Die Ergebnisse werden den Anforderungen an Kommunen im Kontext der kritischen Infrastrukturen gegenübergestellt und mögliche Handlungsbedarfe identifiziert.
In der Untersuchung zeigte sich, dass in 37,5 Prozent der Berichte die Anforderungen an einen IT-Grundschutz laut GPA und in 25 Prozent der Berichte die wesentlichen Anforderungen erfüllt werden. Damit wird für rund 63 Prozent ein IT-Grundschutz angegeben. Keine Gefährdungen wurden in weiteren 28 Prozent der Berichte angegeben. Damit haben rund 90 Prozent der untersuchten Kommunen eine positive Bewertung durch die GPA erhalten. Empfehlung ist hier, die Arbeiten an IT-Sicherheitskonzepten fortzuführen sowie die bestehenden Konzepte zu bündeln und einheitlich zu dokumentieren. Rund drei Prozent der Kommunen arbeiten bereits an einer Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).
In über sechs Prozent der Berichte wurden konkrete Gefährdungen aufgezeigt und in weiteren sechs Prozent eine unzureichende Sicherheitsorganisation. Den Schwerpunkt bilden mit rund 41 Prozent aller Berichte fehlende oder unzureichende Vorgaben zur Notfallvorsorge trotz vorhandener IT-Grundschutzmaßnahmen. In über sechs Prozent wird die Erstellung einer Informationssicherheitsleitlinie empfohlen. Knapp 16 Prozent wird empfohlen, einen IT-Sicherheitsbeauftragten zu verankern.

Kritische Infrastrukturen in zwei Bereiche unterteilt

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und das Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes nehmen keinen direkten Bezug auf Kommunen, sondern adressieren die kritischen Infrastrukturen (KRITIS) im Allgemeinen. Die kritischen Infrastrukturen wurden ausgehend vom Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) in zwei Teilbereiche gegliedert: Den Bereich UP KRITIS als öffentlich-private Kooperation der Betreiber kritischer Infrastrukturen und den Bereich UP BUND für den Bereich Staat und Verwaltung. In diesem Umfeld wurden zahlreiche Dokumente und Leitfäden geschaffen, wobei der Bereich UP BUND noch keine gesetzlichen Anforderungen an Kommunen veröffentlicht hat.
Folgende vom BSI und vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe veröffentlichte Dokumente nehmen Bezug auf Kommunen: Im Jahr 2005 ist ein Dokument mit Empfehlungen für Unternehmen zum Schutz kritischer Infrastrukturen mit Blick auf Basisschutzkonzepte erschienen. 2007 erschien der Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsstrukturen. Die

Nationale Strategie zum Schutz kritischer Infrastrukturen, die so genannte KRITIS-Strategie, wurde im Jahr 2009 veröffentlicht. Im Jahr 2011 wurde zum einen die Cyber-Sicherheitsstrategie für Deutschland und zum anderen der Leitfaden für Unternehmen und Behörden zum Schutz kritischer Infrastrukturen mit Blick auf Risiko- und Krisen-Management herausgegeben. Die Abschätzung der Verwundbarkeit gegenüber Hochwasserereignissen auf kommunaler Ebene (Verwundbarkeitsassessment) und die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung datieren aus dem Jahr 2013. Im darauffolgenden Jahr schließlich erschien die Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen und es wurde die UP KRITIS Öffentlich-Private Partnerschaft zum Schutz kritischer Infrastrukturen institutionalisiert.

Kommunen sind wichtige Bausteine in der KRITIS-Kette

Eine Auswertung der Dokumente zeigt, dass aktuell keine direkten verbindlichen Vorgaben für Kommunen vorliegen. Allerdings gibt es indirekte Verknüpfungen, die im Falle einer Verbindung mit einer Institution, die unter die gesetzlichen Anforderungen fällt, auch die Kommunen in diesen gesetzlichen Anforderungsrahmen rücken. So ist es in der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung der Fall. Die tägliche Arbeit über das Sicherheitsgateway mit Systemen der Landes- oder Bundesbehörden würde diese Verknüpfung beispielsweise herstellen.
Daneben zeigt die Analyse, dass Kommunen als Unterstützer zum Schutz kritischer Infrastrukturen gesehen werden und somit einen wichtigen Baustein in der KRITIS-Kette darstellen. Das BSI schreibt hierzu: „Kommunen sind von einem möglichen Ausfall von kritischen Infrastrukturen unmittelbar betroffen. Daher bezieht die KRITIS-Strategie neben Bund und Ländern explizit auch die kommunale Ebene ein, wenn es darum geht, den Schutz kritischer Infrastrukturen zu fördern und in ihren Zuständigkeitsbereichen umzusetzen.“
Ein Informationssicherheitsmanagement-System (ISMS) kann die bereits in den Kommunen vorhandenen IT-Sicherheitsmaßnahmen weiter ausbauen und für die größtenteils fehlenden Vorgaben zur Notfallvorsorge einen konzeptionellen Rahmen bilden. Ein solches System lässt sich nach und nach ausbauen, um einen einheitlichen Sicherheitsstandard in der Kommune im Kontext der KRITIS zu gewährleisten. Die Grundwerte des ISMS nach BSI IT-Grundschutz entsprechen ebenfalls den Anforderungen nach § 10 Absatz 2 des nordrhein-westfälischen Landes-datenschutzgesetzes (DSG), wonach die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten ist.
Die 32 veröffentlichten Berichte entsprechen rund acht Prozent der 396 Kommunen in Nordrhein-Westfalen. Die Untersuchung ist somit zwar nicht repräsentativ, allerdings gibt sie einen kleinen Einblick in die Ausgangslage und den Handlungsbedarf der Kommunen.

()

Dieser Beitrag ist in der November-Ausgabe von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Nordrhein-Westfalen, Gemeindeprüfungsanstalt Nordrhein-Westfalen