

11.10.2019
Drucksache 167/19

Abschluss einer öffentlich-rechtlichen Vereinbarung über die Bestellung eines gemeinsamen IT-Sicherheitsbeauftragten

Gremium	Sitzungsdatum	Beschlussstatus	Beratungsstatus
Kreisausschuss	04.11.2019	Empfehlungsbeschluss	öffentlich
Kreistag	05.11.2019	Entscheidung	öffentlich

Organisationseinheit	Steuerungsdienst
Berichterstattung	Kreisdirektor Mike-Sebastian Janke

Budget	01	Zentrale Verwaltung
Produktgruppe	01.01	Gesamtsteuerung und Finanzwirtschaft
Produkt	01.01.01	Gesamtsteuerung

Haushaltsjahr	2020 ff	Ertrag/Einzahlung [€]	
		Aufwand/Auszahlung [€]	ca. 33.000

Beschlussvorschlag

Dem Abschluss einer öffentlich-rechtlichen Vereinbarung über die Bestellung eines gemeinsamen IT-Sicherheitsbeauftragten im Rahmen der interkommunalen Zusammenarbeit mit den kreisangehörigen Städten und Gemeinden wird zugestimmt.

Sachbericht

Eine öffentliche Verwaltung ohne IT ist heute undenkbar, denn nahezu alle Geschäftsprozesse der Verwaltung und die Dienstleistungserbringung für die Bürgerinnen und Bürger sind von einer einwandfrei funktionierenden Informationstechnik abhängig. Durch die zunehmende Durchdringung des Alltags mit Informationstechnologien und die voranschreitende Digitalisierung entstehen Chancen, aber auch neue Risiken und Bedrohungslagen z. B. durch Cyber-Kriminalität. Das Problem liegt dabei in der Kombination wachsender Gefährdung mit zunehmender Abhängigkeit von Informationstechnik.

Angriffe auf öffentliche Einrichtungen und Krankenhäuser haben in den vergangenen Jahren zugenommen. Ein besonders pressewirksames Beispiel war der Cyber-Angriff auf das Lukaskrankenhaus in Neuss in 2016, der einen Schaden in Millionenhöhe verursachte. Das Lukaskrankenhaus hat in der Folge in Sicherheitstechnik investiert und zusätzliche Mitarbeiter im Bereich der IT-Sicherheit eingestellt. Das Bundesamt für Sicherheit in der Informationstechnik warnt in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2018“ vor einer steigenden und vielfältigeren Anzahl von Bedrohungen.

Behörden verwalten sensible Daten von Bürgerinnen und Bürgern und stellen daher ein interessantes Ziel für Cyber-Kriminelle dar. Diese Daten sind schützenswerte Güter, für deren Sicherheit die IT bereits heute eine Vielzahl an Schutzmaßnahmen (Firewalls, Virenschutz, Authentifizierung etc.) einsetzt und Sicherheitsstandards laufend erhöht.

Die Rolle des IT-Sicherheitsbeauftragten wird in der Regel derzeit durch die Leitung der IT wahrgenommen. Der Sinn eines IT-Sicherheitsbeauftragten ist jedoch, gerade diese Funktion nicht mit dem Alltagsgeschäft zu vermischen, sondern eine unabhängige Instanz einzurichten, um Interessenskonflikten vorzubeugen. Diese Vorgehensweise empfiehlt im Übrigen auch das Bundesamt für Sicherheit in der Informationstechnik in seinem Bericht „BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise“.

Nach dem BSI-Standard 100-2 kommt dem IT-Sicherheitsbeauftragten die Rolle des Ansprechpartners und Koordinators für Informationssicherheit zu. Informationssicherheit soll die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gewährleisten. Dadurch lassen sich vertrauliche Informationen vor Gefahren wie unbefugtem Zugriff oder Manipulation schützen.

Der BSI-Standard 100-2 (IT-Grundschutz-Vorgehensweise) beschreibt die Zuständigkeit und Aufgaben wie folgt:

„Der IT-Sicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution. Die Hauptaufgabe des IT-Sicherheitsbeauftragten besteht darin, die Behörden- bzw. Unternehmensleitung bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und diese bei der Umsetzung zu unterstützen. Seine Aufgaben umfassen unter anderem:

- *der Informationssicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,*
- *die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,*
- *die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,*
- *die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,*

- *der Leitungsebene und dem IS-Management-Team über den Status quo der Informationssicherheit zu berichten,*
- *sicherheitsrelevante Projekte zu koordinieren,*
- *Sicherheitsvorfälle zu untersuchen und*
- *Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren.“*

Der IT-Sicherheitsbeauftragte ist dabei Hauptansprechpartner bei allen Aspekten der Informationssicherheit; er/sie koordiniert die Aufgabe und treibt sie innerhalb der Verwaltung voran. Er ist der Behördenleitung direkt unterstellt und berichtet an diese. Somit ist die Unabhängigkeit von anderen Organisationseinheiten in der Verwaltung gewährleistet.

Im konkreten Fall wären die ersten Arbeitsschritte des IT-Sicherheitsbeauftragten:

- die Analyse des Status quo der IT-Systeme z. B. der Netzinfrastruktur, der Server- und Client-Systeme, der Serverräume und der bisherigen organisatorischen Regelungen zur IT-Sicherheit,
- die Erarbeitung einer Sicherheitsrichtlinie (allgemeine Sicherheitsziele sowie Strategie zur Erreichung der Ziele),
- Erstellung einer allgemeinen Sicherheitskonzeption sowie Konzepten zu unterschiedlichen Aspekten der Informationssicherheit (Anforderung bei Einführung neuer Soft- und Hardwareprodukte, Virenschutz, Internetnutzung etc.).

Die positiven Erfahrungen mit dem gemeinsamen Datenschutzbeauftragten haben zu den Überlegungen geführt, interkommunale Zusammenarbeit auch bei dem IT-Sicherheitsbeauftragten anzustreben.

Folgende Städte und Gemeinden haben neben dem Kreis Unna in der Folge ihr Interesse an einer Zusammenarbeit erklärt:

- Stadt Bergkamen
- Gemeinde Bönen
- Gemeinde Holzwickede
- Stadt Kamen
- Stadt Lünen
- Stadt Selm
- Kreisstadt Unna
- Stadt Werne

Die Kreisstadt Unna hat sich bereiterklärt, gemeinsam für die o. g. Behörden die Aufgabenträgerschaft für den IT-Sicherheitsbeauftragten wahrzunehmen und hierfür Ressourcen im Umfang von 1,0 VZÄ bereitzustellen.

Die der Kreisstadt Unna entstehenden Personalaufwendungen werden durch die teilnehmenden Kommunen erstattet. Die Gesamtaufwendungen werden auf Grundlage des KGSt-Berichts „Kosten eines Arbeitsplatzes“ berechnet. Der Aufwand wird nach der Anzahl der vollzeitverrechneten Planstellen des jeweils aktuellen Stellenplans des Kreises und der teilnehmenden Städte und Gemeinden verteilt.

Auf Grundlage der Planstellen des Jahres 2019 ergibt sich folgende Kostenverteilung:

Behörde	VZÄ Planstellen	Kostenanteil
Kreis Unna	1.010,26	33.655 €
Stadt Bergkamen	378	12.593 €
Gemeinde Bönen	95	3.165 €
Gemeinde Holzwickede	130,45	4.346 €
Stadt Kamen	430,85	14.353 €
Stadt Lünen	843,15	28.088 €
Stadt Selm	148,84	4.958 €
Kreisstadt Unna	492,84	16.418 €
Stadt Werne	173	5.763 €

Anlage

Öffentlich-rechtliche Vereinbarung über die Bestellung eines gemeinsamen IT-Sicherheitbeauftragten