Cyberangriffe und Datensicherheit in öffentlichen Netzwerken und Dateninfrastrukturen in Deutschland

Bernd W. Wirtz/Jan C. Weyerer

In den letzten Jahren haben Cyberangriffe und Datensicherheit in Wirtschaft, Politik und Verwaltung zunehmend an Bedeutung gewonnen. Trotz des erheblichen Bedeutungsanstiegs gibt es in der Wissenschaft bislang kaum umfassende empirische Studien darüber, wie die öffentliche Verwaltung Cyberangriffe auf öffentliche Netzwerke und Dateninfrastrukturen wahrnimmt und diese bewältigt. Ziel dieses Beitrags ist es daher auf Basis einer solchen Studie den Status quo der Datensicherheit in der öffentlichen Verwaltung in Deutschland zu beschreiben und dabei insbesondere relevante Einstellungen von IT-Experten aus der öffentlichen Verwaltung zu untersuchen, sowie herauszufinden in welchem Umfang geeignete Maßnahmen zum Schutz sensibler behördlicher Daten implementiert sind. Die Ergebnisse dieser Studie sollen der Verwaltungspraxis helfen eine klare Entwicklungslinie zu entwerfen bzw. verfolgen, um zukünftig den vielfältigen Herausforderungen der Datensicherheit gerecht zu werden und Cyberangriffe erfolgreich abzuwehren.

Einführung

Digitale Informations- und Kommunikationstechnologien (IuK) sind durch ihre sehr dynamische Entwicklung in den letzten Jahrzehnten zu einem integralen Bestandteil der öffentlichen Verwaltung geworden und leisten im Verbund mit kritischen öffentlichen Infrastrukturen einen wichtigen Beitrag für Staat, Wirtschaft und Gesellschaft.[1] Die zunehmende Durchdringung der öffentlichen Verwaltung mit IuK-Technologien hat sich inzwischen in Form des E-Government manifestiert und rückt – angesichts der wachsenden Komplexität und Vernetzung der damit verbundenen IT-Systeme sowie der darin erhobenen und verarbeiteten Daten – gleichzeitig das Thema Informationssicherheit in den Fokus.[2] Die zahlreichen Datenskandale der letzten Jahre – wie beispielsweise die jüngsten Cyberangriffe auf den Deutschen Bundestag[3] oder die Datennetzwerke des Weißen Hauses[4] und des US-amerikanischen Verteidigungsministeriums,[5] sowie die Cyberangriffe im Rahmen der US-Präsidentschaftswahl 2016[6] – belegen nicht nur, dass IT-Systeme öffentlicher Verwaltungen verwundbar sind, sondern auch, dass Cyberangriffe auf letztere sowohl in ihrer Häufigkeit zugenommen haben als auch komplexer, professioneller und zielgerichteter geworden sind.[7]

Das damit verbundene Schadenspotenzial ist von erheblicher Bedeutung und reicht von Identitäts- und Datendiebstahl über Onlinespionage bis hin zur Gefährdung der inneren Sicherheit Deutschlands.[8] Vor diesem Hintergrund existieren erstaunlicherweise bisher so gut wie keine empirischen Ergebnisse zur Datensicherheitslage von öffentlichen Netzen in Deutschland. Im Zuge der fortschreitenden und von der Gesellschaft zunehmend geforderten Modernisierung von Verwaltungsvorgängen, stellen insbesondere diese Entwicklungen die öffentliche Verwaltung vor die große und komplexe Herausforderung eine umfassende IT-Sicherheit

Univ.-Prof. Dr. Bernd W. Wirtz
Inhaber des Lehrstuhls für Informations- und Kommunikationsmanagement an der Deutschen Universität für Verwaltungswissenschaften Speyer

Jan C. Weyerer
Wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Informations- und Kommunikationsmanagement an der Deutschen Universität für Verwaltungswissenschaften Speyer

1 Vgl. Wirtz/Daiser 2015.
2 Vgl. Dawes 2008; Wirtz et al. 2015.
3 Vgl. Thomson Reuters 2015a.
4 Vgl. Thomson Reuters 2015b.
5 Vgl. Thomson Reuters 2015c.
6 Vgl. Thomson Reuters 2017.
7 Vgl. Trend Micro 2015.
8 Vgl. Zhou/Hu 2008.

Verwaltung und Management
23. Jg. (2017), Heft 3, S. 154-159

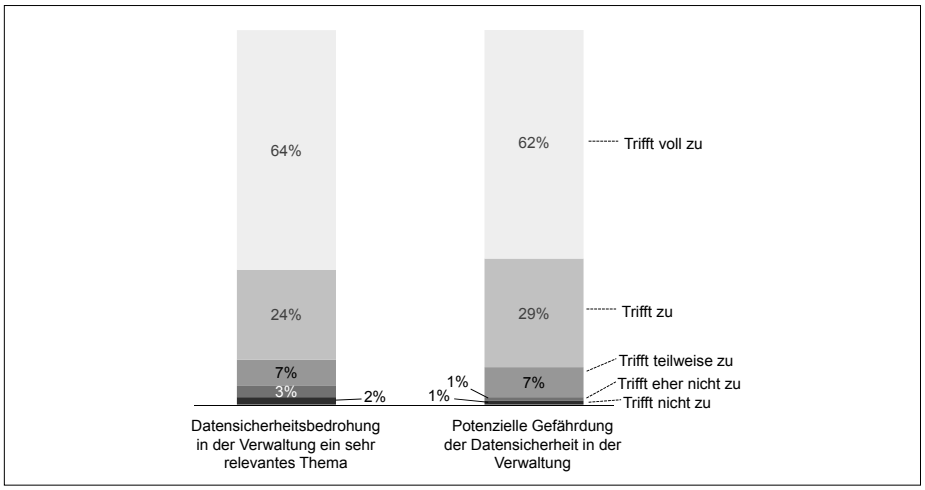

Abb. 1: Relevanz und Gefährdungspotenzial der Datensicherheitsbedrohung in der Verwaltung

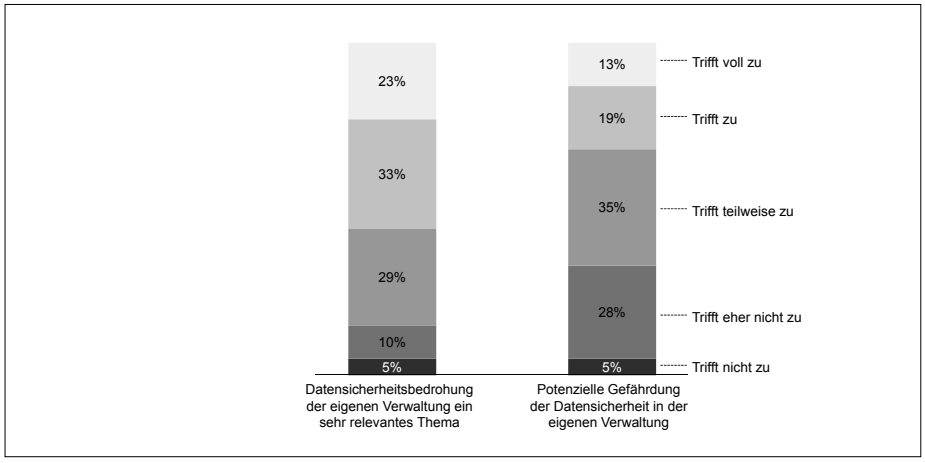

Abb. 2: Relevanz und Gefährdungspotenzial der Datensicherheitsbedrohung in der eigenen Verwaltung

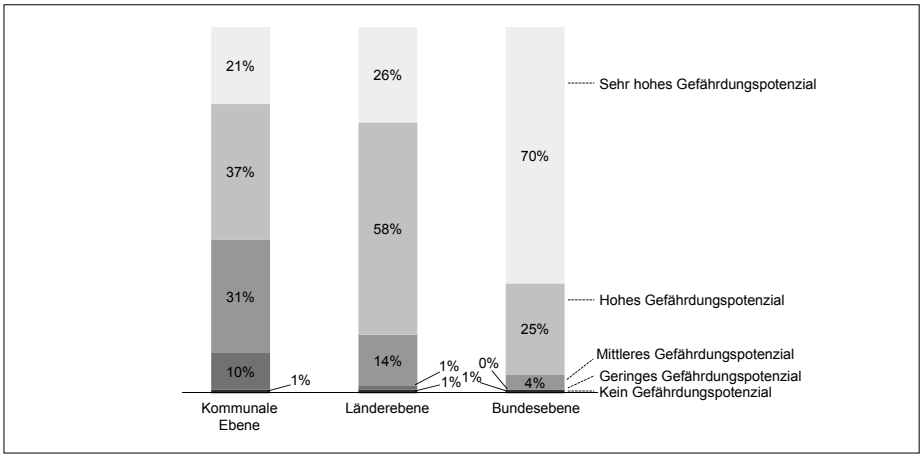

Abb. 3: Gefährdungspotenzial unterschiedlicher Verwaltungsebenen

zu erreichen und somit eine wesentliche Grundlage für ihr Handeln zu gewährleisten. Doch wie nimmt die öffentliche Verwaltung Bedrohungen ihrer IT-Sicherheit und Sicherheit ihrer Daten wahr und wie geht sie damit um? Diese und weitere wichtige Fragen sollen in dieser Studie aus Sicht von IT-Experten aus der öffentlichen Verwaltung beantwortet werden.[9]

Untersuchungsdesign

Die im Folgenden dargestellten Studienergebnisse basieren auf einer deutschlandweiten empirischen Online-Befragung zur Datensicherheit in öffentlichen Netzen. Insgesamt 211 IT-Experten aller Ebenen der öffentlichen Verwaltung nahmen an der Studie teil, wobei das Durchschnittsalter der IT-Experten der öffentlichen Verwaltung bei 50,75 Jahren und ihre Berufserfahrung im IT-Bereich bei durchschnittlich 20,34 Jahren lagen. Die erhobene Stichprobe bestand zu 61 Prozent aus IT-Leitern und zu 39 Prozent aus IT-Mitarbeitern der öffentlichen Verwaltung. Während der Großteil der IT-Experten der öffentlichen Verwaltung (54%) auf Länderebene beschäftigt war, waren gut ein Viertel (24%) auf der Bundesebene und 22 Prozent auf der kommunalen Verwaltungsebene tätig.

Untersuchungsergebnisse

Mit der Expertenbefragung konnten viele interessante Erkenntnisse und Ergebnisse im Hinblick auf die aktuelle Situation der Datensicherheit in der öffentlichen Verwaltung gewonnen werden.[10]

Wahrgenommene Datensicherheitsbedrohung und Gefährdungspotenziale

Ein zentrales Ergebnis ist, dass der Datensicherheitsbedrohung in der öffentlichen Verwaltung allgemein eine überragende Bedeutung zukommt. Demnach stellt für die deutliche Mehrheit (88%) der IT-Experten der öffentlichen Verwaltung die Datensicherheitsbedrohung in der öffentlichen Verwaltung ein sehr relevantes Thema dar und gar 91 Prozent sehen eine potenzielle Gefährdung der Datensicherheit in der öffentlichen Verwaltung (siehe Abb. 1).

Eine entsprechende Beurteilung der Datensicherheitsbedrohung im Hinblick auf die eigene öffentliche Verwaltungsinstitution fällt interessanterweise deutlich geringer aus. Hier schätzt mehr als jeder Zweite (56%) die Datensicherheitsbedrohung als sehr relevant ein und gut ein Drittel (32%) der IT-Experten der öffentlichen Verwaltung sieht die Datensicherheit der eigenen Verwaltung als potenziell gefährdet (siehe Abb. 2).

Insbesondere bei einer Betrachtung unterschiedlicher Verwaltungsebenen zeigt sich ein differenziertes Bild bezüglich des Gefährdungspotenzials. Abbildung 3 ver-

9 Vgl. auch im Folgenden Wirtz/Weyerer 2016.

10 Vgl. auch im Folgenden Wirtz/Weyerer 2016.

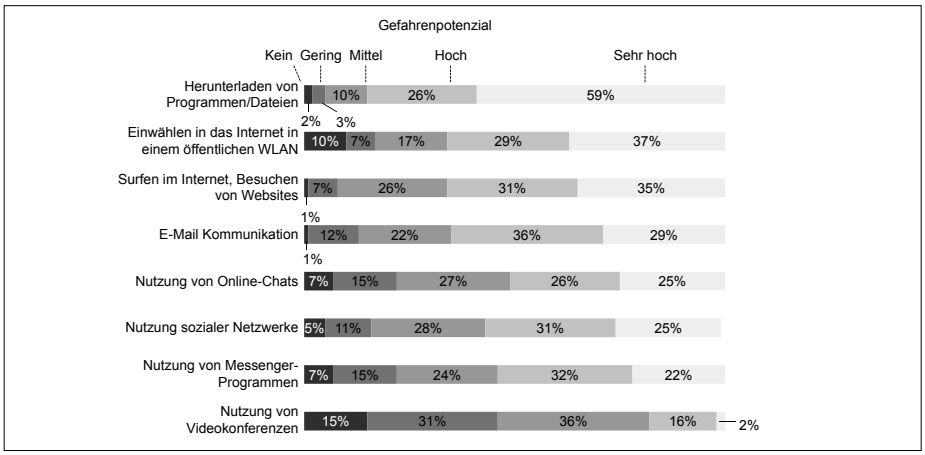

Abb. 4: Gefahrenpotenzial für die Verwaltung durch Tätigkeiten im Internet

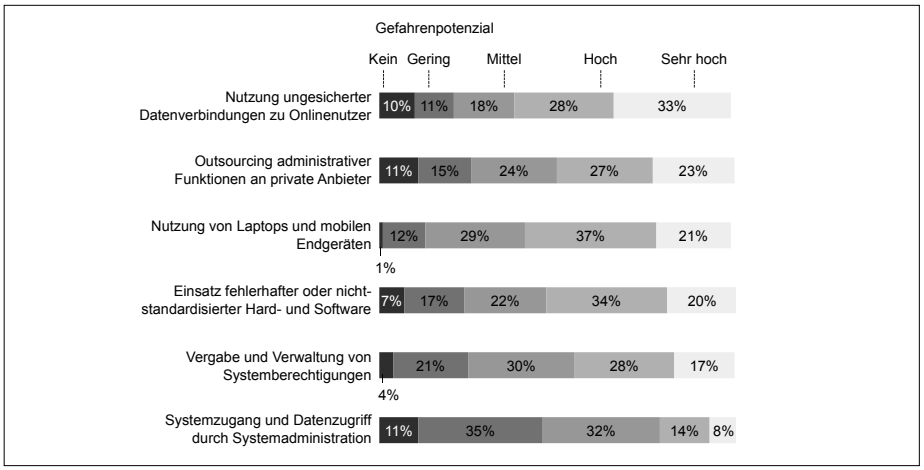

Abb. 5: Gefahrenpotenzial für die Verwaltung durch sonstige organisationsbezogene Aktivitäten

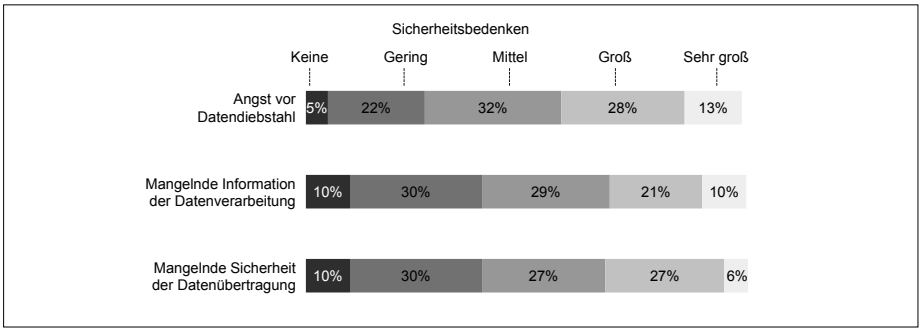

Abb. 6: Sicherheitsbedenken der Verwaltung

anschaulicht, dass mehr als jeder Zweite (58%) ein hohes bis sehr hohes Gefährdungspotenzial auf der kommunalen Ebene sieht, während 84 Prozent der IT-Experten der öffentlichen Verwaltung ein hohes bis sehr hohes Gefährdungspotenzial für die Länderebene angeben und fast alle IT-Experten der öffentlichen Verwaltung (95%) ein solches für die Bundesebene bestätigen.

In diesem Zusammenhang offenbaren sich zahlreiche – teilweise alltägliche – Online- und Offline-Tätigkeiten als interne Gefahrenquellen, die im Handlungsbereich der öffentlichen Verwaltung liegen und somit durch gezielte Maßnahmen im Sinne ihrer Datensicherheit gesteuert werden können.

Ein besonders hohes bis sehr hohes Gefahrenpotenzial geht dabei von Tätigkeiten im Internet aus, wie die Angaben von über der Hälfte der IT-Experten der öffentlichen Verwaltung (58% im Durchschnitt über alle Tätigkeiten in Abbildung 4) bestätigen. Hierzu zählt vor allem das Herunterladen von Dateien, das Einwählen in das Internet in einem öffentlichen WLAN, das Surfen im Internet sowie die Nutzung von E-Mail und sozialer Netzwerke. Abbildung 4 fasst die Tätigkeiten im Internet und das von den IT-Experten der öffentlichen Verwaltung eingeschätzte Gefahrenpotenzial für die öffentliche Verwaltung zusammen.

In Bezug auf die in Abbildung 5 dargestellten sonstigen organisationsbezogenen Aktivitäten erkennt etwa jeder Zweite (48% im Durchschnitt über alle Aktivitäten in Abb. 5) ein hohes bzw. sehr hohes Gefahrenpotenzial für die öffentliche Verwaltung. Diese beziehen sich insbesondere auf die Nutzung ungesicherter Datenverbindungen zu Onlinenutzern, die Verwendung von Laptops und mobilen Endgeräten, den Einsatz fehlerhafter oder nicht-standardisierter Hard- und Software sowie auf das Outsourcing administrativer Funktionen an private Anbieter.

Die Sicherheitsbedenken der IT-Experten der öffentlichen Verwaltung sind zum Teil sehr hoch. Mehr als ein Drittel (35% im Durchschnitt über alle Aspekte in Abb. 6) äußert hier große bis sehr große Sicherheitsbedenken. In Abbildung 6 wird die Intensität der Sicherheitsbedenken seitens der öffentlichen Verwaltung zu verschiedenen Aspekten dargestellt.

Die Sicherheitsbedenken von Bürgern hingegen schätzen die IT-Experten der öffentlichen Verwaltung deutlich größer ein als ihre eigenen. Hier ist knapp die Hälfte der IT-Experten der öffentlichen Verwaltung (46% im Durchschnitt über alle Aspekte in Abb. 7) der Meinung, dass bei den Bürgern große bis sehr große Sicherheitsbedenken vorherrschen. Abbildung 7 gibt hierzu einen Überblick.

Als wichtige Voraussetzung zur Schaffung notwendiger sicherheitsbezogener Rahmenbedingungen ist ein adäquates Risikobewusstsein sowohl der eigenen Behördenleitung als auch der übergeordneten Behörde unerlässlich. Allerdings offenbart hier mehr als jeder Zweite (51%) Schwächen in der öffentlichen Verwaltung, der sich in einem Mangel an sehr hohem Risikobewusstsein auf Seiten der eigenen Behördenleitung und übergeordneten Behörde widerspiegelt. Abbildung

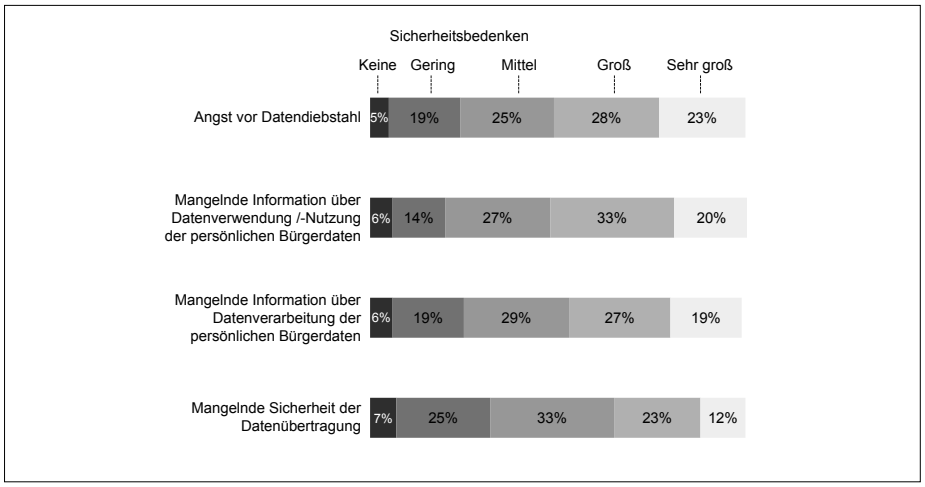

Abb. 7: Sicherheitsbedenken bei Bürgern aus Verwaltungssicht

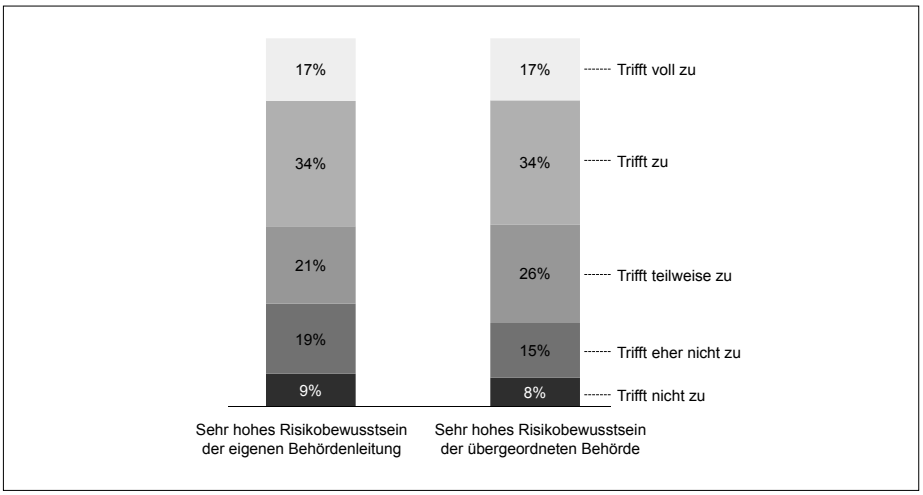

Abb. 8: Risikobewusstsein der eigenen Behördenleitung und übergeordneten Behörde

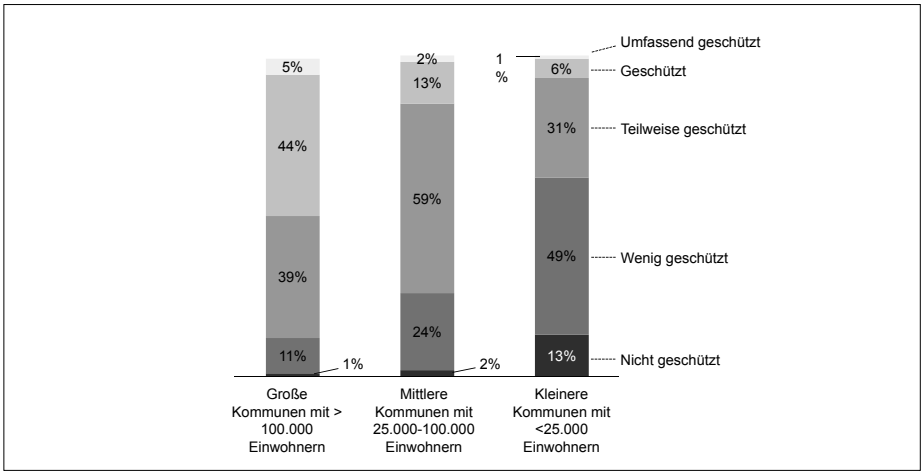

Abb. 9: Datenschutzniveau der Kommunen

8 fasst die Ergebnisse zum Risikobewusstsein übergeordneter Instanzen zusammen.

Wahrgenommener Datenschutz, Schutzmaßnahmen und Ressourcenunterstützung

Im Hinblick auf den Datenschutz bestehen zwischen Kommunen verschiedener Größenordnungen erhebliche Unterschiede, wobei das Datenschutzniveau generell mit zunehmender Kommunengröße zu steigen scheint. Insgesamt weisen die Kommunen jedoch teilweise starke Defizite auf.

Während etwa jeder Zweite (49%) große Kommunen als geschützt oder umfassend geschützt einstuft, sind es für mittlere Kommunen lediglich 15 Prozent und für kleinere Kommunen sogar nur sieben Prozent der IT-Experten der öffentlichen Verwaltung, die der Meinung sind, dass diese geschützt oder umfassend geschützt sind. Abbildung 9 veranschaulicht das wahrgenommene Datenschutzniveau der Kommunen in Abhängigkeit ihrer Größenordnung.

Als potenzielle Maßnahmen des Datenschutzes steht öffentlichen Verwaltungen ein breites Spektrum an Möglichkeiten zur Verfügung, die neben traditionellen Aktivitäten (z.B. Zugangskontrollen, Mitarbeiterschulungen), auch modernere, stärker technisch-orientierte Maßnahmen umfassen (z.B. Sicherheitssoftware, Verschlüsselungstechnologien).

Hierbei zeigt sich zwar, dass nahezu alle öffentlichen Verwaltungen automatische Updates (94%) und diverse Sicherheitssoftware (95% im Durchschnitt über alle vier Softwareaspekte in Abbildung 10) anwenden, gleichzeitig jedoch auch, dass für alle anderen aufgeführten Maßnahmen in vielen öffentlichen Verwaltungen Nachholbedarf besteht (siehe Abb. 10).

Weitere grundlegende Schutzmaßnahmen wie beispielsweise Mitarbeiterschulungen und Zugangskontrollen sind bei 40 Prozent bzw. 55 Prozent (im Durchschnitt über beide Aspekte der Zugangskontrolle in Abbildung 11) der befragten öffentlichen Verwaltungen vorhanden oder vollständig vorhanden und weisen somit ein vergleichsweise geringes Implementierungsniveau auf. Fortgeschrittene Schutzmaßnahmen wie client- und serverseitige Datenverschlüsselung (26% im Durchschnitt über beide Aspekte) oder Standalone-Netzwerke (15%) stellen dagegen eher die Ausnahme dar. In Abbildung 11 sind die unterschiedlichen Datenschutzmaßnahmen und das Ausmaß ihrer Implementierung dargestellt.

Über diese präventiven Schutzmaßnahmen hinaus sind auch reaktive Sicherheitsvorkehrungen von wichtiger Bedeutung, die bei Versagen ersterer bzw. in Notfällen zum Tragen kommen. Hierbei zeigt sich insgesamt ein mittelmäßiges Resultat, da bei etwa ein Drittel (36%)

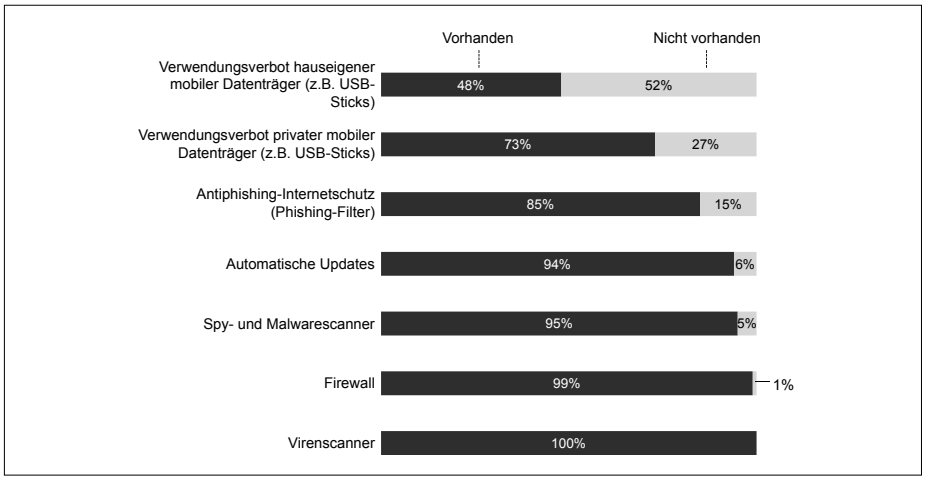

Abb. 10: Schutzmaßnahmen der Verwaltung I

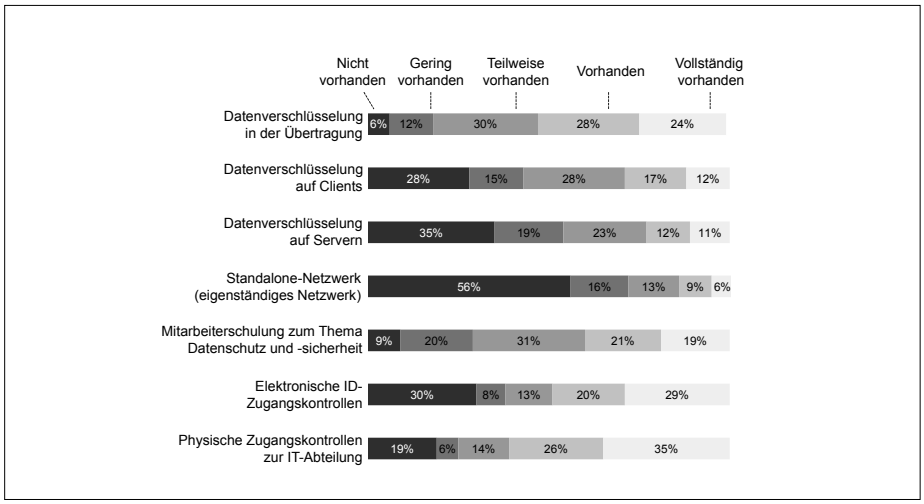

Abb. 11: Schutzmaßnahmen der Verwaltung II

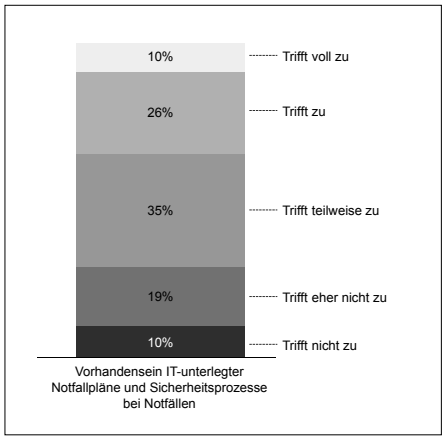

Abb. 12: Notfallmanagement der Verwaltung

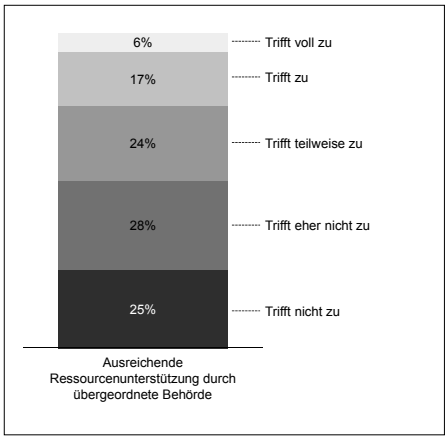

Abb. 13: Ressourcenunterstützung durch übergeordnete Behörde

IT-unterlegte Notfallpläne und Sicherheitsprozesse bei Notfällen vorhanden oder voll vorhanden sind, bei etwa einem anderen Drittel (35%) teilweise vorhanden und bei knapp einem weiteren Drittel (29%) eher nicht oder nicht vorhanden sind. Folglich ergibt sich auch hier für den Großteil der öffentlichen Verwaltungen ein Defizit an Notfallmaßnahmen und somit entsprechender Verbesserungsbedarf.

Übergeordnete Behörden spielen allgemein eine zentrale Rolle bei der Schaffung von Rahmenbedingungen, unter denen sich untergeordnete Behörden bewegen und handeln. Im Speziellen betrifft dies vor allem die Bereitstellung von Ressourcen jeglicher Art (z.B. finanziell oder organisatorisch), die zur Zielerreichung bei Sicherheitsprojekten und zur Implementierung von Schutzmaßnahmen notwendig sind. In diesem Zusammenhang offenbart die Studie erhebliche Schwächen in der öffentlichen Verwaltung. Demnach trifft eine ausreichende Ressourcenunterstützung nur in knapp ein Viertel (23%) aller Fälle zu oder voll zu. Etwa ein weiteres Viertel (24%) bezeichnet eine ausreichende Ressourcenunterstützung nur als teilweise gegeben und für mehr als die Hälfte (53%) der IT-Experten der öffentlichen Verwaltung trifft diese eher nicht oder nicht zu.

Zusammenfassung

Mit der zunehmenden Häufigkeit, Professionalität und Zielgerichtetheit von Cyberangriffen sowie der wachsenden Komplexität und Vernetzung öffentlicher Netzwerke und Dateninfrastrukturen, steht die öffentliche Verwaltung vor vielfältigen Herausforderungen und muss ihre Datensicherheit entsprechend weiterentwickeln und stärken. Vor diesem Hintergrund haben die Studienergebnisse gezeigt, dass die öffentliche Verwaltung der Datensicherheitsbedrohung große Bedeutung beimisst und in ihr ein hohes Gefährdungspotenzial auf allen Ebenen der Verwaltung sieht. Bemerkenswert ist dabei, dass das Gefährdungspotenzial mit der nächsthöheren Verwaltungsebene steigt und auf der Bundesebene das höchste Gefährdungspotenzial besteht.

Darüber hinaus haben sich sowohl alltägliche Tätigkeiten von Verwaltungsmitarbeitern im Internet als auch viele sonstige organisationsbezogene Aktivitäten als potenziell große Gefahrenquellen für die Datensicherheit in der öffentlichen Verwaltung herausgestellt. Zudem offenbaren die Studienergebnisse auch einen Mangel an sehr hohem Risikobewusstsein bezüglich der Datensicherheit bei Behördenleitungen und übergeordneten Behörden. Auch im Zusammenhang mit dem Datenschutzniveau der Kommunen konnten hohe Defizite festgestellt werden. Während große Kommunen als eher geschützt angesehen werden, wird das Schutzniveau kleinerer und mittlerer Kommunen als eher gering eingestuft.

Im Hinblick auf konkrete Maßnahmen zum Datenschutz haben die Studienergebnisse gezeigt, dass grundlegende Sicherheitsvorkehrungen aufgrund ihrer

heterogenen Implementierung in der öffentlichen Verwaltung ein erhebliches Optimierungspotenzial aufweisen und vor allem Nachholbedarf in Bezug auf fortgeschrittene Schutzmaßnahmen sowie das Notfallmanagement besteht. Schließlich hat sich auch gezeigt, dass eine große Mehrheit der öffentlichen Verwaltungen einen Mangel an ausreichender Ressourcenunterstützung im Bereich Datensicherheit durch ihre übergeordneten Behörden wahrnimmt, was auch hier einen entsprechenden Verbesserungsbedarf impliziert.

Insgesamt kann konstatiert werden, dass auf Basis der Einschätzung der IT-Experten der öffentlichen Verwaltung in weiten Teilen eine beunruhigende Datensicherheits- und Datenschutzlage gegen Cyberangriffe in der öffentlichen Verwaltung in Deutschland vorliegt. Die Ergebnisse dieser Studie können Entscheidern in der öffentlichen Verwaltung als wichtige Orientierungshilfe dienen, um zukünftig den vielfältigen Herausforderungen der Datensicherheit gerecht zu werden und Cyberangriffe erfolgreich abzuwehren.

Literatur

Dawes, S.S. (2008): The Evolution and Continuing Challenges of E-Governance, in: Public Administration Review, Nr. 68 (1), S. 86-102. DOI:10.1111/j.1540-6210.2008.00981.x.

Thomson Reuters. (2015a): Cyber Attack on German Parliament Still Active, Could Cost Millions: Media. Berlin, Germany. http://ca.reuters.com/article/technologyNews/idCAKBN0OQ2GA201, Abruf am 26.01.2016.

Thomson Reuters. (2015b): Russian Hackers Reached Sensitive White House Systems: CNN. Washington, DC. http://www.reuters.com/article/ususa-cybersecurity-whitehouse-idUSKBN0MY26420150407, Abruf am 26.01.2016.

Thomson Reuters. (2015c): Pentagon Says Evicted Russian Hackers, Global Cyber Threat Grows. Palo Alto, California. http://www.reuters.com/article/us-usa-pentagon-cyber-idUSKBN0NE29E20150423, Abruf am 26.01.2016.

Thomson Reuters. (2017): Trump Acknowledges Russia Role in U.S. Election Hacking: Aide. Washington, DC. http://www.reuters.com/article/us-usa-russia-cyber-idUSKBN14S0O6, Abruf am 10.01.2016.

Trend Micro. (2015): Report on Cybersecurity and Critical Infrastructure in the Americas. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructureswest-hemisphere.pdf, Abruf am 26.01.2016.

Wirtz, B.W./Daiser, P. (2015): E-Government: Strategy Process Instruments: Textbook for the Digital Society, Speyer. http://berndwirtz.com/downloads/WirtzDaiser_2015_EGovernment.pdf.

Wirtz, B.W./Weyerer, J.C. (2016): Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats, in: International Journal of Public Administration, S. 1-16. DOI: 10.1080/01900692.2016.1242614.

Wirtz, B. W./Weyerer, J. C./Thomas, M.-J./Möller, A. (2015): E-Government Implementation: Theoretical Aspects and Empirical Evidence, in: Public Organization Review, S. 1–20. DOI:10.1007/s11115-015-0330-2.

Zhou, Z./Hu, C. (2008): Study on the E-Government Security Risk Management, in: International Journal of Computer Science and Network Security, Nr. 8(5), S. 208-213.