LUCCA-Seminar zu Cybersecurity in der kommunalen Verwaltung

Moritz Huber M. A.

Kriminalist und Lehrbeauftragter an der HVF

Stellen Sie sich vor, Sie sind Bürgermeisterin oder Bürgermeister und haben nach langwieriger Projektarbeit erfolgreich die Digitalisierung aller hausinternen Aktenbestände abgeschlossen. Strategiepapiere, Abrechnungen, Verwaltungsakten – alle Dokumente liegen nun in elektronischer Form zur effizienten Weiterverarbeitung vor. Dieser Meilenstein deutscher Verwaltungsgeschichte bietet enorme Vorteile: Akten können dezentral bearbeitet werden, der Ressourcenverbrauch wird deutlich reduziert, Prozesse werden beschleunigt und noch vieles mehr. Eine schöne Vorstellung? Ja, eindeutig . . . aber!

Neben dem nahezu unerschöpflich erscheinenden Innovations- und Optimierungspotenzial der Digitalisierung existieren leider auch große Schattenseiten. Ransomware, Phishing oder Advanced Persistent Threats sind Begriffe, die den negativen Aspekten in diesem Kontext einen Namen geben.

Kriminalität wird digital – Erpressung 4.0

Insbesondere Cyberangriffe mittels Ransomware haben in der jüngsten Vergangenheit immer wieder für Aufsehen und Schlagzeilen in der Öffentlichkeit gesorgt. Hierbei handelt es sich um eine besonders bösartige Schadsoftware, die häufig über E-Mail-Anhänge verbreitet wird und bereits für globale Schäden in Millionenhöhe gesorgt hat. Öffnet die adressierte Person den infizierten Anhang, verschlüsselt die Ransomware automatisch alle Daten auf dem Computer des Opfers und im schlimmsten Fall auch alle anderen Daten, die über das angebundene Netzwerk erreichbar sind. Anschließend verlangt das Computerprogramm ein Lösegeld für die (scheinbare) Wiederherstellung der Daten, was neben dem Datenverlust im schlimmsten Falle noch einen weiteren monetären Schaden verursacht. Diese Verfahrensweise gibt der dargestellten Angriffsart auch ihren Namen, der sich aus den englischen Begriffen „Ransom“ (Lösegeld) und „Malware“ (Schadsoftware) zusammensetzt. Allein dieses einzelne Beispiel zeigt, dass auch die organisierte Kriminalität ihre Geschäftsmodelle digitalisiert, denn wir sprechen hier de facto von einer automatisierten „Erpressung 4.0“.

Professionelle Vorbereitungsmaßnahmen werden immer wichtiger

Versuchen wir dieses Szenario in die kommunale Praxis zu übertragen. Was würde wohl ein derartiger Ransomware-Angriff in dem oben angesprochenen Rathaus auslösen, das erst kürzlich alle Akten digitalisiert hat? Die richtige Antwort lautet: Es kommt darauf an! Das Spektrum der möglichen Folgen einer derartigen Attacke reicht von „kaum erwähnenswert“ bis „geschäftskri-

Moritz Huber referiert über die Chancen und Risiken der Digitalisierung

tisch und katastrophal“, je nachdem wie gut die Cybersecurity-Maßnahmen der angegriffenen Kommune im Vorfeld waren. Sofern aktuelle Backups verfügbar sind, ein wirksames Notfallmanagement implementiert wurde, Zuständigkeiten und Verantwortlichkeiten feststehen sowie fachkundiges Personal vorhanden ist, wird sich der Schaden des Vorfalls in Grenzen halten. Wenn nicht, dann geht es der Gemeinde höchstwahrscheinlich wie der bayerischen Stadt Dettelbach und vielen anderen Kommunen, die im Jahr 2016 im Fokus der Kriminellen standen.

Kommunale Verantwortungsträger müssen geschult werden

Da die dargestellte Bedrohung durch Ransomware nur einen kleinen Teilbereich der aktuellen und kommenden Cybergefahren abdeckt und die Digitalisierung der öffentlichen Verwaltung immer weiter voranschreitet, werden zunehmend auch kommunale Führungskräfte und Entscheider stärker mit entsprechenden Fragestellungen konfrontiert. Denn Cybersecurity ist das zentrale Querschnittsthema, wenn es um Digitalisierungsbestrebungen aller Art geht. Grund genug für die Hochschule Ludwigsburg, um dem erkannten Praxisbedarf am Ludwigsburg Competence Centre of Public Administration (LUCCA) mit einem Cybersecurity-Seminar für Nicht-Informatikerinnen und -Informatiker zu begegnen.

Durch die interdisziplinären und behördenübergreifenden Verbindungen des Alumni-Netzwerkes des berufsbegleitenden Master-Studiengangs Public Management konnte auf Initiative von Prof. Dr. Volkmar Kese schnell ein Expertenteam aus unterschiedlichen Bereichen der Landesverwaltung als Referierende für die Veranstaltung gewonnen werden. Bernhard Lacker, Regina Holzheuer und Moritz Huber gaben am 7. Februar 2019 mehr als 20 Teilnehmerinnen und Teilnehmern aus ganz Baden-Württemberg einen praxisorientierten Überblick über die Themenkomplexe „Bedrohungslage im Bereich Cybercrime“, „Chancen und Risiken der Digitalisierung“ sowie „Cybersecurity und Notfallmanagement“.

Das LUCCA-Seminar beschäftigte sich mit der zentralen Fragestellung, wie sich die kommunale Ebene besser vor Cyberangriffen und anderen Gefahren schützen kann. Während vor einigen Jahren noch der Betrieb einer Firewall und eines Virenscanners ausreichte, um sich wirksam gegen die meisten Cyberangriffe abzusichern, können diese beiden Maßnahmen heutzutage nur kleine Bestandteile einer ganzheitlichen Sicherheitsarchitektur sein. Durch die Komplexität und Dynamik des Cybersecurity-Umfelds sollten Kommunen sich dringend mit dem Aufbau eines risikobasierten Informationssicherheitsmanagementsystems (ISMS) beispielsweise auf Basis des BSI IT-Grundschutz oder ISIS12 beschäftigen. Hierbei handelt es sich zwar um einen Meilenstein von herausragender Bedeutung, für sich allein betrachtet reicht er jedoch auch noch nicht aus, um ein angemessenes Schutzniveau zu erzielen. Denn selbst die besten Absicherungsmaßnahmen bieten keine hundertprozentige Sicherheit.

Daher sollten Kommunen zusätzlich noch ein praxisorientiertes IT-Notfallmanagementsystem aufbauen. Auf diese Weise kann im Ernstfall, etwa bei einem geschäftskritischen Cyberangriff, zielgerichtet und strukturiert reagiert werden. Dies ist insbesondere deshalb wichtig, da die Erfahrungen aus der Praxis zeigen, dass IT-Notfälle egal welcher Art bei unvorbereiteten Organisationen immense Schäden anrichten können. Da gerade in diesem Bereich jedoch noch erheblicher Forschungsbedarf besteht, arbeiten derzeit fünf Studierende aus dem Master-Studiengang Public Management der Hochschule Ludwigsburg zusammen mit der Gemeinde Salach (Kreis Göppingen) an einem innovativen Pilotprojekt zur Verbesserung des Status quo. Ziel ist es, langfristig eine skalierbare und übertragbare Systematik zu entwickeln, wie sich Städte und Gemeinden effektiv und effizient auf die Bewältigung von Cyberangriffen vorbereiten können.

Cybersecurity ist mehr als nur Technik!

Abschließend gilt es, ein großes Missverständnis anzusprechen, das immer wieder zu fataler Fehleinschätzung und operativen Problemen führt. Das Themenfeld Cybersecurity ist im öffentlichen Diskurs stark mit technischen Assoziationen behaftet. Hieraus resultieren vielfach sehr einseitig ausgerichtete Einzelmaßnahmen, die aufgrund mangelnder Einbettung in eine gesamtkonzeptionelle Lösung nicht die gesetzten Erwartungen erfüllen. Cybersecurity sollte daher nicht nur aus technischer, sondern zwingend auch aus programmatischer, organisatorischer und personeller Perspektive betrachtet werden. Bei näherer Befassung wird dies schnell deutlich, denn was nützt die beste Technik, wenn kompatible Schnittstellen fehlen, keine aufbau- und ablauforganisatorischen Verantwortlichkeiten festgelegt werden und es niemanden gibt, der damit umgehen kann?

Informatives

Das 2016 gegründete Ludwigsburg Competence Centre of Public Administration (LUCCA) versteht sich als Zentrum für lebenslanges Lernen für Mitarbeiterinnen und Mitarbeiter in der Verwaltung. Neben eigenständigen Kontaktstudien bietet LUCCA weitere, kurzformatige Fortbildungsmöglichkeiten an. Weitere Tagesveranstaltungen zu aktuellen Themen im Ausländer-, Asyl- und Flüchtlingsrecht, im Internati- onales Privatrecht oder der Besteuerung der öffentlichen Hand (mit § 2b UStG) unter www.hs-ludwigsburg.de/lucca

LUCCA
Ludwigsburg Competence Centre of Public Administration
Hochschule Ludwigsburg