5 Safety first: IT-Sicherheit in Kommunen noch immer unterschätzt!

Ob Krankenhäuser, Kammern oder Kommunen, alle waren schon von Cyberattacken betroffen. Setzte in der Vergangenheit ein Trojaner einzelne Produkte oder Arbeitsplätze kurzfristig außer Kraft, verschlüsselt heute Schadsoftware als Ransomware-Angriff ein ganzes System. Wer das Lösegeld nicht bezahlt, kann in den meisten Fällen seine IT neu aufsetzen. Infolge eines solchen Angriffs können Verwaltungen über Wochen lahmgelegt sein.

Die überörtliche Kommunalprüfung zeigte in den Jahren 2021 bis 2023 mehr als 30 Kommunen zahlreiche Handlungsbedarfe in verschiedenen Bereichen der IT-Sicherheit, darunter Notfallmanagement und mobiles Arbeiten, auf. Sie sensibilisierte vor Ort und sprach Empfehlungen für kurzfristig umsetzbare Maßnahmen aus. Auch wenn die geprüften Kommunen schon auf erkennbare Fortschritte blicken können, bleibt die Aufgabe „IT-Sicherheit" dauerhaft herausfordernd.

5.1 Rückblick und Ausgangslage

Die überörtliche Kommunalprüfung verfolgt bereits seit 2016 einen Prüfungsschwerpunkt in den Bereichen Informationstechnologie, Informationssicherheit und Datenschutz. Ziel dieser Prüfungen war und ist es, die Kommunen für die vorgenannten Bereiche zu sensibilisieren und gutes Verwaltungshandeln zu identifizieren. Die bisher durchgeführten Prüfungen[151] zeigten auf, dass es für die Kommunen eine große Herausforderung darstellte, ein angemessenes IT-Sicherheitsniveau herzustellen. In allen Prüfungsfeldern erkannte die überörtliche Kommunalprüfung wesentlichen Nachhol- bzw. Handlungsbedarf. Die Stellungnahmen der Kommunen zu den bisher abgeschlossenen Prüfungen bestätigten die hohe Praxisrelevanz.

Cyber-attacken werden immer häufiger

Schadsoftware (Malware) beeinträchtigte bundesweit bereits etliche Verwaltungen über Wochen bis hin zur völligen Arbeitsunfähigkeit. Nach Angaben des Bundeskriminalamtes (BKA) registrierten deutsche Behörden im Jahr 2022 knapp 137.000 Fälle von Cyberkriminalität. Zudem kalkulierte der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) für das

[151] Die Präsidentin des Niedersächsischen Landesrechnungshofs: Informationssicherheit in Kommunen – Bisher ist es meist gut gegangen (Kommunalbericht 2017, Kapitel 5.10); Informationssicherheit in Kommunen – Externer Sachverstand muss nicht teuer sein (Kommunalbericht 2018, Kapitel 5.7); Verzeichnis von Verarbeitungstätigkeiten und Auftragsverarbeitung – Defizite bei der Umsetzung der EU-DSGVO (Kommunalbericht 2019, Kapitel 5.8); Informationssicherheitsmanagementsysteme und Sensibilisierung von Beschäftigten: Ausbaufähig! (Kommunalbericht 2020, Kapitel 5.4; Hohe Gefahren durch Cyberkriminalität – Kommunen müssen sich besser schützen! (Kommunalbericht 2022, Kapitel 5.5); Baustelle Cybersicherheit – Wie geht es voran? (Kommunalbericht 2023, Kapitel 3.9), zuletzt abgerufen am 24.10.2023.

Jahr 2022 wirtschaftliche Gesamtschäden durch Cyberkriminalität in Höhe von 203 Mrd. Euro, die sich damit gegenüber dem Jahr 2019 verdoppelten.[152]

Leicht anzugreifende Ziele im Fokus

Bei der Beantwortung einer Anfrage[153] führte die niedersächsische Landesregierung zu diesem Thema aus, dass Ransomware[154] nutzende Cyberkriminelle bei der Auswahl ihrer Opfer nicht nach den Kategorien Verwaltung, Wirtschaft oder kritischen Infrastrukturen unterscheiden. Häufig wählen sie leicht anzugreifende sowie kurz- bis mittelfristig finanziell lohnende Ziele aus. Für die Kommunen ergibt sich damit zwingend die Notwendigkeit, den Schutz von Computernetzwerken und Daten fortwährend zu verbessern. Auch die Beschäftigten sind bestmöglich zu sensibilisieren und zu schulen.

Ansicht 26: Cyberangriffe nehmen täglich zu[155]

Angriffe treffen Kommunen mit voller Härte

Wie schnell und wie leicht eine Kommune zum Opfer eines Cyberangriffes wird, zeigt sich am Beispiel der Stadtverwaltung Rodgau in Hessen: Mit einer simplen E-Mail (Malware im Dateianhang) blockierten Cyberkriminelle im Februar 2023 die gesamte technische Verwaltungsabwicklung. Dieser Ransomware-Angriff führte dazu, dass die Stadtverwaltung ihre Arbeit buchstäblich auf Bleistift und Papier umstellen musste. Wochenlang konnten Fachanwendungsverfahren und digitale Leistungen nicht genutzt werden, da die IT von Grund auf neu aufgesetzt werden musste. Auch das bloße Versenden von E-Mails zur Weitergabe behördeninterner Informationen war den Beschäftigten nicht möglich. Die Auswirkungen des Angriffs konnten auch nach mehreren Monaten nicht vollständig eingeschätzt werden.[156]

---

152 Vgl. Wirtschaftliche Gesamtschäden durch Cyberkriminalität im Jahr 2022, zuletzt abgerufen am 27.11.2023.

153 Vgl. Niedersächsischer Landtag, Drs. 18/10132, IT-Sicherheit der kommunalen Verwaltung, zuletzt abgerufen am 10.05.2024.

154 Das BSI teilt mit, dass Ransomware für eine Art von Schadprogrammen stehe, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe werde dann ein Lösegeld (englisch: Ransom) verlangt.

155 Bildnachweis: Sasun Bughdaryan – stock.adobe.com

156 Vgl. Stadt Rodgau - Sachstand nach dem Cyberangriff, zuletzt abgerufen am 20.10.2023.

Noch härter traf es im Oktober 2023 den kommunalen Zweckverband Südwestfalen-IT (SIT) und hierdurch bis zu 153 anhängige Kommunen/Organisationen. Von einem Moment auf den anderen setzte ein Ransomware-Angriff nicht nur die ganze kommunale Verwaltungs-IT Südwestfalens außer Betrieb, die Auswirkungen zeigten sich auch in Teilen Niedersachsens.[157] Viele Kommunen schalteten infolgedessen einen großen Teil oder gar alle ihre IT-Prozesse und Webseiten ab. Soweit es diese Angriffsdimension angeht, dürfte es sich um den bisher größten Cyberangriff auf deutsche Kommunen handeln.[158]

Einfallstor mobiles Arbeiten

Ein weiteres Einfallstor für Cyberkriminalität bietet das mobile Arbeiten vieler Beschäftigter. Die Kommunen bieten vermehrt die Möglichkeit an, von zu Hause aus zu arbeiten. Insbesondere in Folge der Pandemie ist dieses Angebot erstmals eröffnet bzw. beträchtlich ausgeweitet worden. Dabei wurden private Endgeräte genauso wie ungesicherte Speichermedien (z. B. private USB-Sticks) zur dienstlichen Nutzung geduldet. Die Arbeit außerhalb des Büroarbeitsplatzes stellt jedoch weitergehende Anforderungen an die IT-Sicherheit. Die Gefahr eines Datenmissbrauchs oder einer unzulässigen Einflussnahme durch Dritte ist bei mobilem Arbeiten höher, da der Arbeitgeber/Dienstherr nur eingeschränkte Kontroll- und Einflussmöglichkeiten hat.

5.2 IT-Basis-Check der überörtlichen Kommunalprüfung

Die Vielzahl von Hackerangriffen verdeutlicht die Notwendigkeit, den Schutz von Computernetzwerken und Daten zu intensivieren. Die Kommunen müssen daher angemessene Abwehrmaßnahmen ergreifen und die Beschäftigten gezielt sensibilisieren.

Basis Check bei 31 Kommunen

Die überörtliche Kommunalprüfung hat den Stand der IT-Basis-Absicherung in den Kommunen im Rahmen der Prüfungsreihe „Informationssicherheit“ in den Jahren 2021 bis 2023 bei insgesamt 31 Kommunen[159] untersucht. Geprüft wurden kleinere Kommunen in der Größenordnung zwischen 6.800 und 24.300 Einwohnerinnen und Einwohnern. Für den Basis-Check wählte die überörtliche Kommunalprüfung verschiedene Schwerpunkte wie Sicherheitsmanagement, Zugang zu IT-Systemen oder Notfallmaßnahmen aus. Ziel war es herauszufinden, ob die Kommunen die

---

157 Dieser Angriff wirkte sich auch vereinzelt auf Standesämter in den Landkreisen Celle und Uelzen aus, die die Fachanwendung „AutiSta“ verwenden.

158 Vgl. Cyberangriff auf Südwestfalen IT, zuletzt abgerufen am 23.11.2023.

159 Im Jahr 2021 wurden die Gemeinde Nordstemmen, die Flecken Delligsen und Salzhemmendorf sowie die Samtgemeinden Emlichheim, Herzlake und Schüttorf geprüft. Im Jahr 2022 wurden die Gemeinden Dörverden, Hambühren und Wendeburg, der Flecken Langwedel sowie die Samtgemeinden Ahlden, Bothel, Hankensbüttel, Lachendorf, Schwarmstedt und Suderburg geprüft. Im Jahr 2023 wurden die Städte Burgwedel, Langelsheim, Pattensen, Rehburg-Loccum, Ronnenberg sowie Sarstedt, die Gemeinde Cremlingen, der Flecken Aerzen, die Samtgemeinden Boldecker Land, Hattorf am Harz, Ostheide, Sachsenhagen, Scharnebeck, Salzhausen und Sittensen geprüft.

notwendigen Maßnahmen zur Sicherung ihrer Systeme, aber auch ihrer dort hinterlegten Daten, ergriffen. Auch das „Worst-Case-Szenario“ beleuchtete die überörtliche Kommunalprüfung, in dem sie der Frage nachging, ob die Kommunen die wichtigsten Geschäftsprozesse bei einem kompletten Ausfall der IT-Infrastruktur – auch bei nur kurzfristigen Unterbrechungen – zeitnah wiederaufnehmen können.

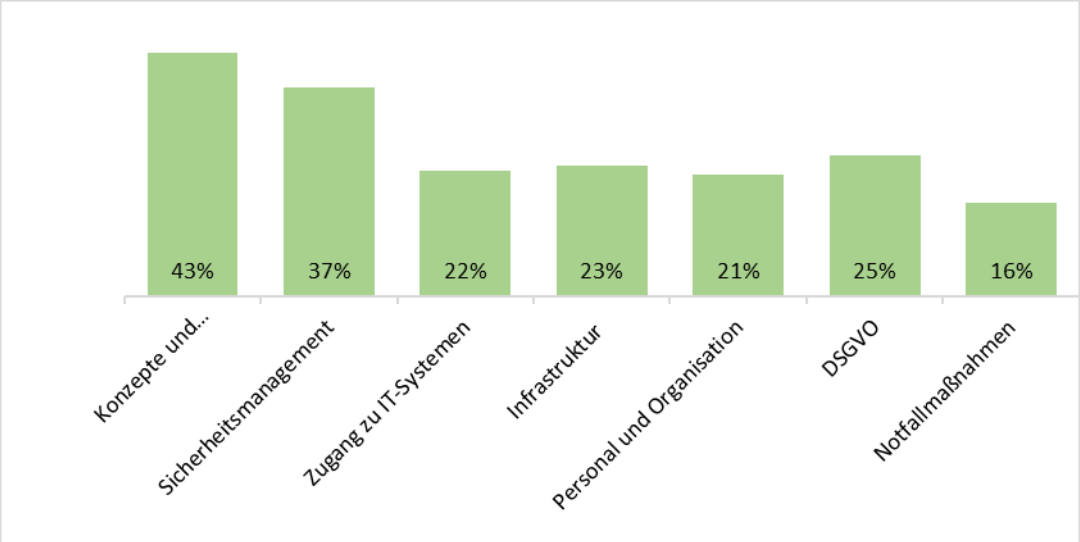
Ziel: Mindest-sicherheits-niveau

Um eine fundierte Datenbasis zu erhalten, entwickelte die überörtliche Kommunalprüfung für den IT-Basis-Check einen Fragenkatalog.[160] Dieser basierte im Wesentlichen auf dem IT-Grundschutz Profil Basis-Absicherung Kommunalverwaltung, den Standards 200-1 bis 200-4 des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) sowie des Informations-Sicherheits-Management-Systems in 12 Schritten (CISIS 12). Zudem passte die überörtliche Kommunalprüfung den Fragenkatalog im Laufe der Prüfungsreihe kontinuierlich an, um aktuellen Entwicklungen Rechnung zu tragen.

5.3 Prüfungsreihe deckt Lücken auf

Im vorliegenden Kommunalbericht fasst die überörtliche Kommunalprüfung die durch die Prüfungsreihe gewonnenen Erkenntnisse zusammen.

Sie stellte für die geprüften Kommunen in den einzelnen Prüffeldern der Informationssicherheit folgende Handlungsbedarfe fest:



Ansicht 27: Durchschnittliche Handlungsbedarfe im IT-Basis-Check 2021 - 2023

160 Vgl. Fragenkatalog zum IT-Basis-Check der überörtlichen Kommunalprüfung.

Mängel in den Konzeptionen und dem Sicherheitsmanagement überwiegen

Vornehmlich traten beim IT-Basis-Check Mängel in den Bereichen Konzeption und Vorgehensweisen sowie Sicherheitsmanagement auf. Es fehlten im Wesentlichen Strategien, Ziele, Leitlinien und Dokumentationen, die notwendig und gefordert sind. Die überörtliche Kommunalprüfung stellte zudem fest, dass in fast allen geprüften Kommunen im Bereich Sicherheitsmanagement eine behördenspezifische Leitlinie zur Informationssicherheit fehlte. In dieser sollen Schutzziele wie Vertraulichkeit, Integrität und die Verfügbarkeit der Daten definiert und die jeweilige Zielerreichung beschrieben sein.

Häufig begegneten die Kommunen der überörtlichen Kommunalprüfung zu diesem Themenfeld mit Aussagen, dass sie Dokumentationen zur IT-Sicherung nicht bräuchten und für solche Aufgaben auch keine Zeit fänden. Unter der Prämisse „Was man lebt, braucht man nicht dokumentieren“, sei dem Thema bereits ausreichend Raum gewidmet worden. Einigen Kommunen waren zudem die zu erfüllenden Anforderungen, wie das Erstellen einer Informationssicherheitslinie, nicht bekannt.

Weiterhin ergab die Prüfungsreihe fortwährenden Handlungsbedarf für die Einführung eines funktionierenden Managementsystems für Informationssicherheit (ISMS) in allen geprüften Kommunen. Dieses System regelt u. a. die Gebäudesicherheit, Schutzkonzepte gegen Schadsoftware, Zugangsberechtigungen oder Notfallpläne.

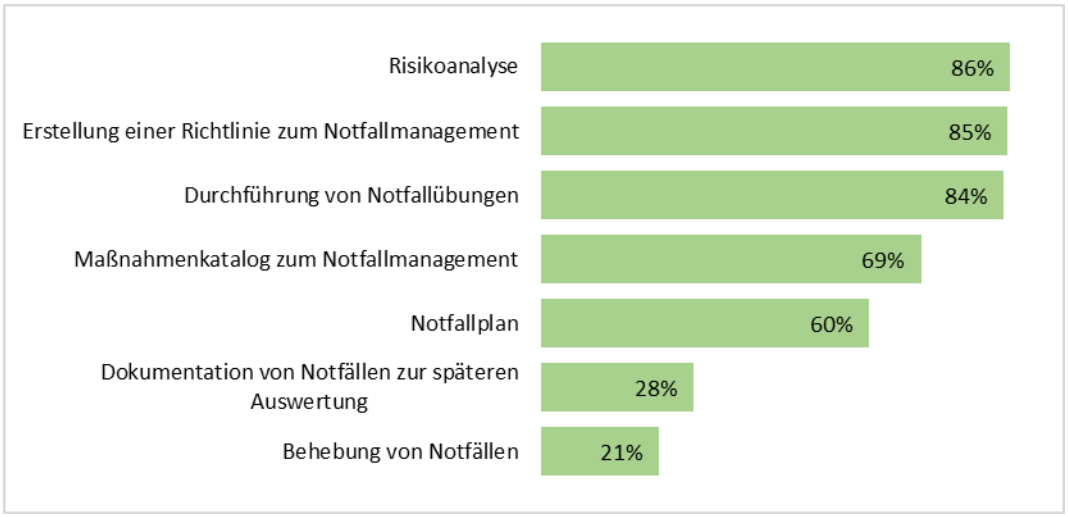
Ob Hinweisschilder auf Serverräume oder Stromverteilungskästen, die durch den Serverraum verlaufende Hauptwasserleitung oder fehlende Alarmsysteme: Dies sind Mängel, die in verschiedenen geprüften Kommunen nicht nur vorlagen, sondern im Ernstfall auch zu gravierenden Problemen führen können. Auch die Nutzung des Serverraums als Lagerfläche für anderweitige Zwecke sollte künftig unterbleiben. Positiv ist hervorzuheben, dass die geprüften Kommunen in Bezug auf Firewall, Virenschutz und WLAN regelmäßig gut aufgestellt waren. Handlungsbedarfe ergaben sich des Öfteren bei der Nutzung externer Anschlüsse, wie USB-Ports oder Kartenlesern. USB-Ports können beispielsweise als Einfallstore für Hackerangriffe, Datendiebstahl und Malware-Infektionen dienen. Allein mit einem USB-Stick kann die IT-Sicherheit umgangen und Schadprogramme auf dienstliche Rechner übertragen werden.

5.4 IT-Notfallmanagement – Regelungen für den Ernstfall

Notfallmanagement: Problemfeld Nr. 1

Vertiefend befasste sich die überörtliche Kommunalprüfung in den Jahren 2021 und 2022 mit dem IT-Notfallmanagement. Dieses soll sicherstellen, dass eine Behörde in allen IT-Notfalllagen ihren Betrieb aufrechterhalten kann und die Geschäfts- und Handlungsfähigkeit weiterhin gegeben ist. Elemente des IT-Notfallmanagements sind dabei nicht nur regulierende Maßnahmen, wie die Erstellung von Richtlinien. Bei der

Entwicklung eines IT-Notfallmanagements sind vor allem präventive Maßnahmen zu ermitteln, umzusetzen und wiederholt zu üben. Die Prüfungsreihe zeigte deutliche Handlungsbedarfe auf:



Ansicht 28: Handlungsbedarfe im Vertiefungsthema Notfallmanagement

Die Mehrheit der Kommunen führten im Vorfeld keine Risikoanalysen durch. Dadurch identifizierten und bewerteten sie mögliche Gefahren nicht. Auch Richtlinien zum Notfallmanagement sowie konkrete Notfallpläne fehlten. Einige der geprüften Kommunen begannen aber bereits, erste Vorkehrungen zu treffen.

Die überwiegende Mehrzahl der geprüften Kommunen führten keine Notfallübungen durch. Sie nahmen sich dadurch die Möglichkeit, durch simulierte Trainings und Tests die Reaktion auf IT-Notfälle zu überprüfen und Handlungsbedarfe zu erkennen. Auch die IT-Notfallkarte war nur in wenigen Kommunen bekannt und ausgehängt. Die Notfallkarte gibt den Beschäftigten bei IT-Notfällen Orientierungshilfe durch wichtige Verhaltenshinweise, benennt Ansprechpartner und trägt allein schon durch ihre optische Wirkung zur Sensibilisierung der Beschäftigten bei.

Ansicht 29: IT-Notfallkarte[161]

Die überörtliche Kommunalprüfung empfiehlt daher allen niedersächsischen Kommunen, ihr IT-Notfallmanagement sowie die im Ernstfall anstehenden Notfallmaßnahmen zu überprüfen und ggf. zu ergänzen. Der seitens der überörtlichen Kommunalprüfung abrufbare Fragenkatalog bietet dafür eine gute Hilfestellung.[162] Vor allem gilt es präventiv zu handeln, um Störungen und damit Schäden durch den Ausfall von Informationstechniken oder den Datenverlust zu vermeiden. Alle Kommunen sollten in ihre Überlegungen auch Monitoring-Systeme, u. a. zur Einbrucherkennung sowie Feuchtigkeitsüberwachung, im Serverraum einbeziehen. Gleiches gilt für Maßnahmen, die vor kurzfristigen Stromausfällen schützen, z. B. unterbrechungsfreie Stromversorgungssysteme.

5.5 Zusätzliche Sensibilisierung durch Landesprogramm „B-Hard“

Angesichts der vermehrten Cyberangriffe, auf die auch die überörtliche Kommunalprüfung in ihren unterschiedlichen Veröffentlichungen wiederholt hinwies,

---

161 Vgl. BSI. IT-Notfallkarte.
162 Vgl. Fußnote 160.

ergriff auch das Land verschiedene Maßnahmen zum Schutz der kommunalen IT-Systeme. So bot das Innenministerium seit Juni 2022 niedersächsischen Kommunen die kostenfreie Durchführung von Cybersicherheitsanalysen (Programm „B-Hard“) durch eine auf IT-Sicherheit spezialisierte Firma an. Diese untersuchte, ob die Kommunen die technischen und organisatorischen Anforderungen an eine angemessene Absicherung gegen Bedrohungen aus dem Cyberraum erfüllen. Rd. 190 Kommunen nutzten in den Jahren 2022 und 2023 dieses Angebot.[163]

Zeitgleich führte die überörtliche Kommunalprüfung ihre Prüfungsreihe Informationssicherheit durch. Das dazu ausgewählte Prüfungsspektrum ging über die Cybersicherheit hinaus. Informationssicherheit umfasst auch Gefahren, die nicht aus dem Internet drohen, wie Social Engineering (Ausspähen von Beschäftigten – Phishing) oder der physische Schutz der Hardware (Stichwort: sichere Serverräume).

Ansicht 30: Optimale Serverräume sorgen für Sicherheit[164]

B-Hard und IT-Basis-Check ergänzen einander

Vier seitens der überörtlichen Kommunalprüfung untersuchten Kommunen nahmen auch an der Sicherheitsanalyse „B-Hard“ teil. Sie berichteten, dass sich die B-Hard Prüfung vertiefend mit der technischen Analyse der vorgefundenen Infrastruktur durch den Einsatz von Scan-Software befasste. Eine Prüfungsmethodik, die der gesetzliche Auftrag des NKPG nicht vorsieht. Die überörtliche Kommunalprüfung hätte ergänzend dazu durch ihre gezielte Fragebogenerhebung mit Vor-Ort-Erörterung der Ergebnisse zeitnahe und konkrete Hilfestellungen sowie Lösungsansätze zur

163 Im Jahr 2024 werden 40 weitere Kommunen die Möglichkeit einer solchen Sicherheitsanalyse nutzen können.
164 Bildnachweis: evannovostro – stock.adobe.com

Informationssicherheit angeboten. Beide Maßnahmen zeigten den Kommunen umfängliche Handlungsempfehlungen zur Verbesserung ihrer Cybersicherheit auf.

5.6 Ausfallkosten durch Cyberangriffe

Schäden können immens sein

Das BSI führt im Jahresbericht 2021 aus, dass von der Entdeckung einer Infektion mit einer Ransomware bis zur Bereinigung der Systeme und vollständigen Wiederherstellung der Arbeitsfähigkeit durchschnittlich 23 Tage vergehen.[165] Vielfach ist den Kommunen nicht bekannt, welche Schäden in diesem oder einem evtl. längeren Zeitraum durch Cyberangriffe entstehen und welche Kosten damit verbunden sein können.

Zu den möglichen zum Teil erheblichen Folgen eines IT-Ausfalls zählen insbesondere

- Personalausfallkosten (Produktivverluste),
- Kosten für das Wiederherstellen von Daten,
- Kosten für das Wiederbeschaffen von verlorenen Daten,
- Kosten für externe Dienstleister (technisch und juristisch),
- Sachkosten für erforderlichen Ersatz von Hard- oder Software,
- Regressforderungen,
- Einnahmeausfälle und
- Reputationsverluste (z. B. bei Auftragsverarbeitung, IKZ).

Häufig sahen sich angegriffene Kommunen mit Lösegeldforderungen von bis zu siebenstelligen Summen konfrontiert, damit die Daten wieder entschlüsselt werden.[166] Bei der Ermittlung potentieller Schadenshöhen ist es nach Auffassung von Bitkom nicht möglich, konkrete Zahlen zu nennen.[167] Dies begründete Bitkom damit, dass sich die Schadenshöhe anhand des konkreten Angriffs sowie dem betroffenen Unternehmen bzw. der betroffenen Behörde bemesse. Hierbei seien so viele Faktoren zu berücksichtigen, dass nur eine Einzelfallanalyse entsprechende Schäden zuverlässig bezifferbar mache. Insbesondere seien alle Kosten (ausgenommen der Produktivverluste) schwer fassbar, da sie von Art und Umfang des „Notfalls“ abhängig seien. Konkrete Zahlen zu diesen Kosten sind in bisher bekannten Fällen von Cyberangriffen auf Kommunen nicht veröffentlicht worden.

---

165 Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2021, Seite 14 zuletzt abgerufen am 24.10.2023.

166 Vgl. Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen, zuletzt abgerufen am 01.11.2023.

167 Vgl. Leitfaden Kosten eines Cyber-Schadensfalles, 2016 S. 4; Welche Kosten entstehen bei einem Cyberangriff?, zuletzt abgerufen am 26.10.2023.

Der Landkreis Anhalt-Bitterfeld[168] schätzte drei Monate nach dem Cyberangriff die Kosten bereits im sechsstelligen Bereich. Diese Schätzung wurde weit übertroffen. Insgesamt sind dem Landkreis bislang Kosten von etwa zwei Millionen Euro im Zusammenhang mit dem Cyberangriff entstanden.[169]

Die Größenordnung möglicher Personalausfallkosten kann hingegen abgeschätzt werden, da sie vom prozentualen Zeitanteil der IT-Einbindung des jeweiligen Arbeitsplatzes abhängig ist. Die Bezifferung zu erwartender Produktivverluste stellen zwar nur einen Aspekt der möglichen Ausfallkosten dar. Zugleich wird greifbar, wie essentiell die im Rahmen der Prüfungsreihe untersuchten Abwehrmaßnahmen sein können.

Um ein vergleichbares Bild der möglichen Personalausfallkosten[170]
(= Produktivverluste) in den Verwaltungen zu erhalten, betrachtete die überörtliche Kommunalprüfung die Produktivverluste der allgemeinen Verwaltung. In den geprüften Kommunen lagen die potenziellen Personalausfallkosten damit bei:

Prüfungsjahr	Ø Einwohner (-in)	Ø Ausfall je Tag	Ø lt. BSI 23 Tage
2021	11.583	8.837,24 €	203.256,52 €
2022	10.186	10.576,84 €	243.267,32 €
2023	13.718	18.441,03 €	424.143,75 €

Tabelle 5: Durchschnittliche Personalausfallkosten

Generell gilt: Je mehr Beschäftigte IT-Arbeitsplätze nutzen und je fortgeschrittener die Technisierung ist, desto höher sind die voraussichtlichen Kosten des Produktivitätsausfalls. Zugleich steigt auch der Bedarf an angemessenen Schutzmaßnahmen.

168 Erstmals rief am 09.07.2021 mit dem Landkreis Anhalt-Bitterfeld eine deutsche Kommune wegen eines Hackerangriffs den Katastrophenfall aus, der erst im Februar 2022 – nach 207 Tagen – beendet werden konnte. Anfang Juli 2022, ein Jahr nach dem Vorfall, war die Rekonstruktion der Daten nach Schätzungen zu 80-90 % abgeschlossen. Vgl. Cyberangriff auf Landkreis Anhalt-Bitterfeld, zuletzt abgerufen am 02.11.2023.

169 Vgl. Ein Jahr nach dem Erpressungstrojaner - Anhalt-Bitterfeld spürt noch die Folgen, zuletzt abgerufen am 26.10.2023.

170 Als Berechnungsgrundlage nutzte die überörtliche Kommunalprüfung die jeweils durch die KGSt veröffentlichten Berichte „Kosten eines Arbeitsplatzes“.

5.7 Mobiles Arbeiten kann zur Sicherheitslücke werden

Auch mobiles Arbeiten benötigt Sicherheits-standards

Das mobile Arbeiten[171] wurde 2020, insbesondere durch die COVID-19-Pandemie, für die meisten Kommunen und ihre Beschäftigten in kürzester Zeit notwendig. Während die IT-Sicherheitsinfrastruktur in den Kommunen in der Regel ein gewisses Schutzniveau aufwies, änderte sich dies durch die Verlagerung der Arbeitsplätze aus den Büros in die heimischen vier Wände deutlich. Die Kommunen mussten daher trotz dieser besonderen Situation sicherstellen, dass an den häuslichen Arbeitsplätzen entsprechende Vorkehrungen getroffen werden.

Ansicht 31: Cyberangriffe meiden auch das mobile Arbeiten nicht[172]

Die überörtliche Kommunalprüfung stellte positiv fest, dass alle Kommunen bereits einen sicheren Zugang zum behördlichen Netzwerk für mobiles Arbeiten bereitstellten. Dies ist zwingend erforderlich, um einen geschützten Datentransfer vom mobilen Arbeitsplatz zur Dienststelle zu gewährleisten. Ohne diese Verbindung können Daten leicht von dritter Seite abgefangen und für kriminelle Zwecke missbraucht werden.

Unterschiedlich regelten die Kommunen jedoch Sicherheitsaspekte wie Zugriffs- und Zutrittsschutz, Umgang mit Speichermedien und Verschlüsselung. Dabei stellte ein besonderes Risiko die Möglichkeit zur Nutzung privater PCs dar, die bei einigen Kommunen erlaubt bzw. geduldet war. Der Dienststelle war es unter diesen Umständen kaum möglich, die IT-Sicherheit zu gewährleisten. Vor allem gilt dies bei

171 Die Bezeichnung „Mobiles Arbeiten“ wird als Oberbegriff für die Arbeitsformen Homeoffice, Telearbeit, mobiles Arbeiten oder auch alternierende Telearbeit verwendet.

172 Bildnachweis: Rawf8 – stock.adobe.com

der Verwendung nicht sicherer Passwörter, verwalteter Virensoftware oder dem Einsatz ungesicherter privater Speichermedien.

Arbeiten von überall möglich

Die Prüfung zeigte auch, dass einzelne Kommunen mobiles Arbeiten auf den häuslichen Arbeitsplatz beschränkten, während andere ortsunabhängiges Arbeiten erlaubten. Hierbei besteht ein gravierendes Sicherheitsrisiko, wenn unsichere öffentliche WLAN-Verbindungen, z. B. auf Dienstreisen in Zügen, genutzt werden.

Festzuhalten bleibt, dass die geprüften Kommunen auch zukünftig mobiles Arbeiten anbieten werden. Die virtuelle Zusammenarbeit mit Beschäftigten am mobilen Arbeitsplatz bietet aber auch weiterhin Einfallstore für Cyberkriminelle. Aus Sicht der überörtlichen Kommunalprüfung ist es unerlässlich, klare, verlässliche und der Sicherheit entsprechende Regelungen zu treffen. Soweit noch nicht umgesetzt, sollten die Kommunen für ein vergleichbares Sicherheitsniveau beim mobilen Arbeiten sorgen.

5.8 Und welche kommunalen Einrichtungen sind noch betroffen?

Auch kommunale Unternehmen sind gefährdet!

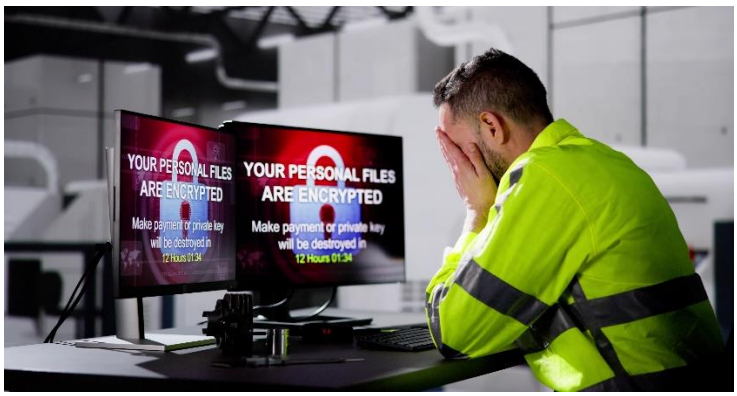
Kommunale Unternehmen nehmen häufig wichtige Aufgaben der Daseinsvorsorge wahr. Hierbei handelt es sich u. a. um Unternehmen bzw. Eigenbetriebe des Gesundheitswesens oder der Energiever- sowie Abwasserentsorgung. Diese Unternehmen und Organisationen werden als Operatoren von kritischen Infrastrukturen (KRITIS) eingestuft. Sie können damit auch interessante Ziele für Cyberangriffe sein.

Die Europäische Union hat als Reaktion auf die steigenden Bedrohungen durch Cyberangriffe die neue Richtlinie NIS 2[173] erlassen. Danach müssen Betreiber kritischer Infrastruktur[174] rechtliche Maßnahmen zur Steigerung ihres Gesamtniveaus zur Cybersicherheit treffen. Sie haben beispielsweise eine Risikoeinschätzung zur Ermittlung und Bewertung potenzieller Angriffe und möglicher IT-Sicherheitsrisiken durchzuführen. Zugleich ist auch ein Sicherheitsmanagementsystem gefordert sowie eine Sensibilisierung der Beschäftigten.

---

173 Vgl. NIS-2-Richtlinie.

174 Grundsätzlich unterliegen alle Unternehmen, die als Betreiber kritischer Infrastrukturen gelten, dieser Richtlinie. Ausgenommen sind jedoch Unternehmen, die weniger als 50 Beschäftigte haben und deren Jahresumsatz bzw. Jahresbilanzsumme maximal zehn Millionen Euro beträgt.



Ansicht 32: Auch kommunale Unternehmen sind Opfer von Cyberattacken[175]

Vor diesem Hintergrund sollten alle Kommunen darauf hinwirken, dass auch die von ihnen gegründeten Unternehmen und Ausgliederungen diesem Schutzniveau Rechnung tragen.

Schule = kommunale IT-Sicherheit

Ferner hat in den letzten Jahren die digitale Unterrichtsversorgung und -gestaltung an niedersächsischen Schulen verstärkt zugenommen. Waren es früher einzelne Unterrichtsräume bzw. Computer, die mit einem Netzwerk bzw. WLAN verbunden waren, verfügen heute viele Klassenräume über digitale Tafeln und die Lehrerschaft über Dienstnotebooks. Ab der 8. Jahrgangsstufe findet häufig der Unterricht über Tablets statt, die mit dem Schulnetzwerk verbunden sind.

Dieser Medienaufwuchs erfordert neben digitalen Unterrichtskompetenzen auch eine funktionierende und leistungsfähige IT-Infrastruktur. Für diese digitale Schulinfrastruktur sind die Kommunen nach derzeitiger Rechtslage zuständig.[176] Neben sämtlichen sächlichen Kosten, dem Aufbau und der Unterhaltung dieser digitalen Infrastruktur haben sie vornehmlich auch für die IT-Sicherheit an den Schulen zu sorgen. Dies bedeutet, dass die aufgezeigten Handlungsfelder auf kommunaler Verwaltungsebene auch in allen Schulen berücksichtigt werden müssen.

---

175 Bildnachweis: Andrey Popov – stock.adobe.com

176 Vgl. § 108 Abs. 1 NSchulG.

Ansicht 33: Medialer Unterricht nimmt deutlich zu[177]

Ob freigeschaltete USB-Ports, Nutzung von privaten Mobilfunktelefonen der Schülerinnen und Schüler zur Übertragung von Daten auf digitale Unterrichtstafeln oder Schultablets, die eventuell auch für private Zwecke eingesetzt werden: Mit allen Optionen gehen Sicherheitsrisiken einher, die das Gesamtgebilde „Schul-IT“ mit Viren oder Schadsoftware belasten können.

Aufgrund der Feststellungen der Prüfungsreihe kann die überörtliche Kommunalprüfung auch in den vorgenannten Bereichen vergleichbare Risiken nicht ausschließen. Sie rät den Kommunen, die Schul-IT frühzeitig hinsichtlich eventueller Handlungsbedarfe zu prüfen.

5.9 Fazit

Der Weg ist das Ziel!

Die kommenden Jahre werden für die Kommunen von entscheidender Bedeutung sein, wenn es darum geht, sich den Herausforderungen der Digitalisierung zu stellen und deren Chancen für sich zu nutzen. Dabei ist das Risiko, Opfer einer Cyberattacke zu werden, heute höher denn je. Die steigenden Anforderungen an die IT-Sicherheit stellen insbesondere kleinere Kommunen vor große Herausforderungen.

Die Prüfungsreihe Informationssicherheit deckte mit dem IT-Basis-Check nicht nur in den geprüften Kommunen Lücken auf, sondern sorgte mit ihren Berichten generell für Orientierung und Hilfestellung. Die in der Prüfungsreihe aufgezeigten Handlungsfelder ermöglichen allen Kommunen, entsprechende Vorkehrungen zu treffen.

---

177 Bildnachweis: David Fuentes – stock.adobe.com