BIGS | Essenz

Brandenburgisches Institut für GESELLSCHAFT und SICHERHEIT

Cyberangriffe auf deutsche Kommunen im Jahr 2021

Esther Kern

Nummer 19 · März 2022

1. EINLEITUNG

2021 war für die IT-Verwaltungen deutscher Kommunen kein gutes Jahr. Schlagzeilen wie „Cyberangriff mit Schadsoftware „DeepBlueMagic"‚[1] „Staatsanwaltschaft ermittelt nach IT-Angriff auf Schwerin"‚[2] „Kein Normalbetrieb mehr in diesem Jahr"[3] waren in regelmäßigen Abständen zu lesen. Der bekannteste und wohl auch schwerwiegendste Cybervorfall im letzten Jahr war mit Sicherheit der Angriff auf den Landkreis Anhalt-Bitterfeld. Mit Anhalt-Bitterfeld wurde zum einen auch die Diskussion über den Schutz kommunaler IT-Infrastrukturen neu entfacht und zum anderen wurde darüber debattiert, wer eigentlich welche Verantwortlichkeiten hat und Hilfe leisten soll/muss, wenn ein Katastrophenfall nach einem Cyberangriff wie in Bitterfeld ausgerufen wird.

Das Kommando Cyber- und Informationsraum der Bundeswehr oder wie von der AG KRITIS[4] vorgeschlagen, ein Cyberhilfswerk vergleichbar mit dem Technischen Hilfswerk? Fakt ist jedoch, dass kommunale wie auch Länderstrukturen sehr schnell an ihre Grenzen geraten, wenn sie von einem Cyberangriff betroffen sind und oftmals Unterstützung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder wie in diesem Fall von der Bundeswehr brauchen, die eigentlich nur in Extremfällen zuständig sind.

Bisher gibt es keine staatliche, bundesweite Stelle, die (erfolgreiche) Cyberangriffe auf Kommunen systematisch erfasst und analysiert. Selbst auf Länderebene ist dies zum größten Teil wohl nicht der Fall – zumindest nicht öffentlich bekannt. Eine Umfrage von Zeit Online und dem Bayrischen Rundfunk im Juli 2021 zum Thema Ransomware unter den Bundesländern ergab, dass nur ein Teil in der Lage oder willens war, konkrete

1 Vgl. Die Zeit (2021).
2 Vgl. Grüner (2021).
3 Vgl. NDR (2021).
4 Vgl. Biselli (2020).

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Antworten zu liefern. So gaben u. a. Nordrhein-Westfalen und Berlin an, dass entsprechende Erpressungsversuche nicht erfasst werden.[5] Auch diese vorliegende Kurzstudie kann dies nicht leisten, da sie sich auf öffentlich zugängliche Quellen stützt. Trotzdem wird hier der Versuch gewagt, etwas Licht in die Black Box Cyberangriffe auf kommunale Verwaltungen zu werfen. Insbesondere wird analysiert, mit welcher Art von Cyberangriffen deutschen Kommunen im Jahr 2021 umgehen mussten, ob sich bestimmte Charakteristika festmachen lassen, wie hoch im Durschnitt die Kosten waren und wie lange es durchschnittlich gedauert hat bis Kommunen wieder voll arbeitsfähig waren.

Teil der Untersuchung sind (erfolgreiche) Cyberangriffe auf 27 deutsche Kommunen im Zeitraum von Januar bis Dezember 2021. Explizit wird sich hier auf die öffentlichen, kommunalen Verwaltungen fokussiert. Damit sind klassischerweise Gemeinde-, Stadt- und Kreisverwaltungen gemeint, die Bürgerdienste und -services für die in ihrem Gebiet lebenden Personen erbringen. Dies geschieht, um eine bessere Vergleichbarkeit herzustellen.

Für eine systematische Erfassung, um eine Gesamtlage der Bedrohungen für den als kritische Infrastruktur (KRITIS) definierten Bereich Staat und Verwaltung zu erlangen, müssten neben den Verwaltungen auch Cyberangriffe auf Institutionen der Legislative und Judikative betrachtet werden. Außerdem müssten Landes- wie Bundesbehörden mitberücksichtigt werden. Zudem sollten auch Angriffe auf kommunale Versorgungswerke, wie z. Bsp. die Stadtwerke oder Stadtreinigung miteinbezogen werden.

Das BSI kam im Lagebericht 2021 zu dem Urteil, dass die „IT-Sicherheitslage in Deutschland insgesamt […] im aktuellen Berichtszeitraum angespannt bis kritisch"[6] war. Eine Herausforderung wird dabei vor allem auf Grund der unterschiedlichen Formen der sogenannten cyber-kriminellen Erpressungen gesehen sowie kritischen Schwachstellen wie die in den Microsoft Exchange Servern. Es muss daher betont werden, dass jenseits von den hier besprochenen Fällen, stark davon auszugehen ist, dass es zahlreiche weitere versuchte Cyberangriffe auf deutsche, kommunale Verwaltungen gab, die jedoch dann erfolgreich von entsprechenden Schutzmaßnahmen wie u.a. Virenschutzprogrammen und Firewalls geblockt und/oder nicht offiziell kommuniziert wurden.

Um beurteilen zu können, wie angespannt die Lage in deutschen, kommunalen Verwaltungen tatsächlich ist, bräuchte es weitere Informationen, z. Bsp. wie viele Phishingangriffe haben kommunale Verwaltung durchschnittlich pro Tag, welche Sicherheitsmaßnahmen sind inzwischen zum Standard geworden, aber auch wie bereiten sich deutsche Kommunen auf den Fall eines erfolgreichen Cyberangriffes vor? Gibt es z. Bsp. *Business Continuity* Pläne und damit verbundene Wiederherstellungskonzepte? Diese und weitere Informationen wären vonnöten, um sich ein umfassendes Bild zu machen.

Was ist Sicherheit?

„Sicherheit [lässt] sich als Funktion aus Bedrohung und Schutz verstehen. Das Sicherheitsniveau korreliert typischerweise positiv mit den Schutzleistungen und negativ mit der Bedrohung." (Bretschneider et. al. (2020)).
Sicherheit ist somit die Summe aus Bedrohungen einerseits und diesen Bedrohungen entgegenwirkenden Schutzleistungen andererseits.
Ein bestimmtes Sicherheitsniveau leitet sich dabei erst von den einzusetzenden Schutzleistungen im Verhältnis zur Bedrohung ab.
Ressourcen werden solange in Schutzleistungen fließen, bis das Maß an Sicherheit, unter Beachtung der Budgetrestriktion, ein für das Individuum oder die Gesellschaft zufriedenstellendes Maß erreicht hat.

5 Vgl. Biermann (2021).
6 Bundesamt für Sicherheit in der Informationstechnik (2021, S. 9).

Foto © 512r / Shutterstock.com

Trotz dieser nicht (öffentlich) vorhandenen Informationen, muss jedoch davon ausgegangen werden, dass die Lage mindestens angespannt bis kritisch ist. Denn, deutsche Kommunen stehen unter dem Druck ihre Dienstleistungen zu digitalisieren, wie es auch das Onlinezugangsgesetz[7] vorsieht. Gleichzeitig nimmt die Bedrohungslage zu. Auf diese Bedrohungslage muss mit entsprechenden präventiven Maßnahmen reagiert werden, dies würde jedoch den Einsatz von vermehrten finanziellen wie personellen Ressourcen bedeuten. Denn bei konstanten Sicherheitsausgaben nimmt die Sicherheit bei gleichzeitig zunehmender Bedrohungslage ab. In Zeiten angespannter Budgets, insbesondere auch aufgrund der Covid-19-Pandemie, sind jedoch steigende Ausgaben im Bereich IT-Sicherheit kein leichtes Unterfangen.

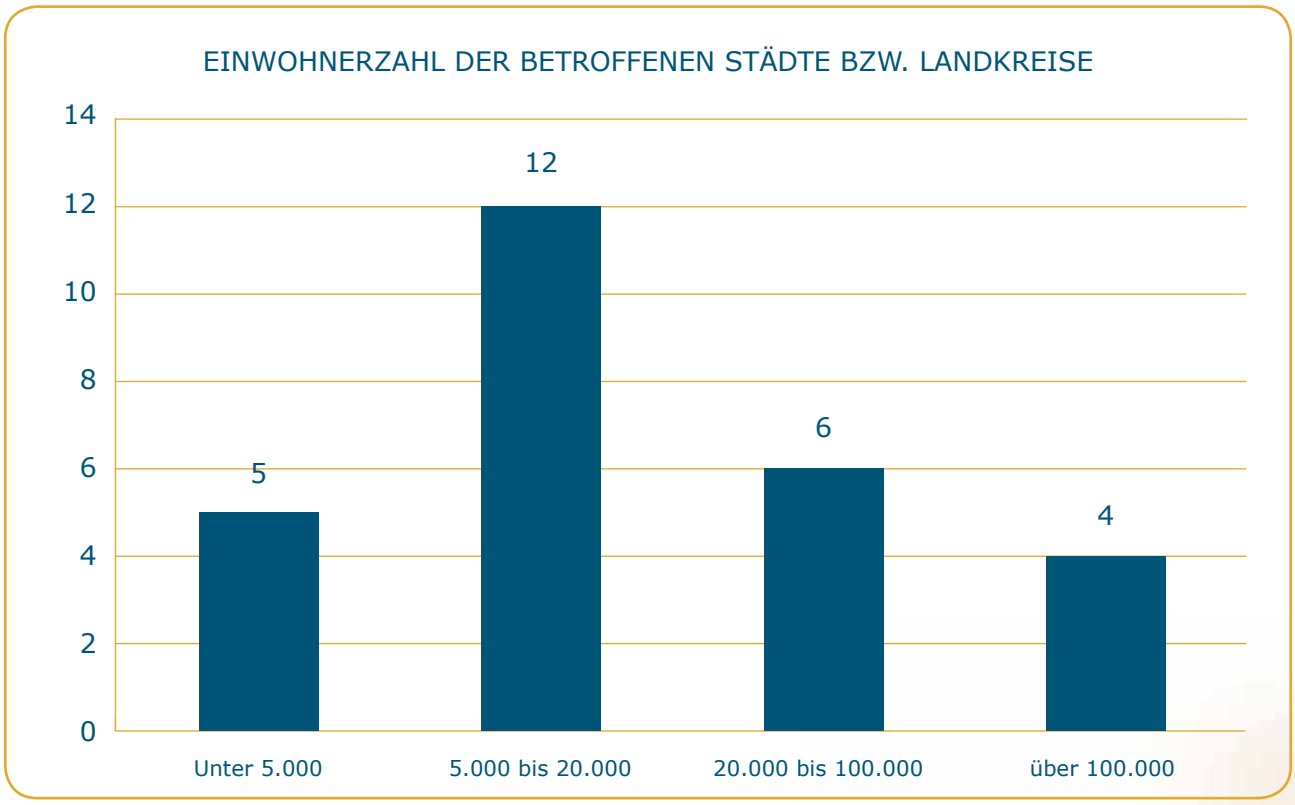
Zudem handelt es sich bei IT-Sicherheit im ersten Moment, um etwas abstraktes und diffuses. Wenn die Abwägung ist, ob Geld in die Renovierung von Schulen oder in die IT-Sicherheit der Verwaltung investiert werden soll, fällt die Entscheidung in vielen Kommunen auf die Schule. Zudem ist die Investition und Umsetzung von Maßnahmen im Bereich IT-Sicherheit nicht das Thema, welches sich besonders eignet, um im Wahlkampf auf Stimmenfang zu gehen. Doch die Grundprämisse für alle Digitalisierungsprojekte sollte bei allen Herausforderungen sein, dass Digitalisierung mit Sicherheit Hand in Hand gehen muss. Vor allem dann, wenn man wie Kommunen tagtäglich mit sensiblen Daten arbeitet und viele Schnittstellen zu Bürger und Bürgerinnen aufgrund der angebotenen Verwaltungsdienstleistungen hat. Zudem sind Kommunen die Stellen in Deutschland, die finanzielle Hilfen wie Sozialleistungen auszahlen.

7 Das Onlinezugangsgesetz (OZG) bzw. das „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen" wurde 2017 verabschiedet. Das Gesetz verpflichtet Bund, Länder wie auch Kommunen ihre Verwaltungsleistungen bis spätestens Ende 2022 auch elektronisch über entsprechende Portale anzubieten sowie diese zu einem Verbund miteinander zu verknüpfen. Jedoch hinken alle Verwaltungsorgane weit zurück und es ist absehbar, dass diese Deadline verfehlt wird. Der Normenkontrollrat stellte in seinem Gutachten „Monitor Digitale Verwaltung #6" im September 2021 fest, dass es bis Ende 2022 nicht zu schaffen sei die 575 OZG-Leistungsbündelungen umzusetzen (für mehr Details siehe Nationaler Normenkontrollrat (2021)).

CYBERANGRIFFE UND DEUTSCHE KOMMUNEN

Der folgende Abschnitt analysiert 27 Cyberangriffe auf deutsche Kommunen und Landkreise im Zeitraum von 01.01.2021 bis 31.12.2021.[8] Es zeigt sich, dass im Jahr 2021 Kommunen bzw. deren Verwaltung jeglicher Größe angegriffen wurden. Schwerpunktmäßig waren aber Kommunen mit Einwohnerzahlen unter 100.000 betroffen. Dies ist nicht ganz verwunderlich, da größere Städte auch in aller Regel mehr personelle wie finanzielle Ressourcen zur Verfügung haben, um diese entsprechend in IT-Sicherheitsstrukturen zu investieren.

Abbildung 1: Einwohnerzahl der betroffenen Städte bzw. Landkreise



Quelle: Eigene Darstellung.[9]

Abbildung 2 zeigt die Art der Angriffe. In über 50% der Fälle im Jahr 2021 waren die Kommunen von Ransomware betroffen. Hier ist jedoch auch zu erwähnen, dass sieben der 15 Ransomware-Fälle auf einen Angriff der Server der Schweriner IT- und Sicherheitsgesellschaft (SIS) und Kommunalservice Mecklenburg (KSM)[10] zurückgeführt werden können. Hierdurch wurde eine Kettenreaktion ausgelöst.[11] Doch auch schwerwiegende Schwachstellen wie die der Microsoft Exchange Server[12] sowie die Sicherheitslücke Log4J,[13] die im Dezember 2021 bekannt wurden, führten zu Cyberangriffen auf Kommunen.

8 Eine Übersicht der Cyberangriffe findet sich online auf der Webseite des BIGS: https://www.bigs-potsdam.org/app/uploads/2022/03/Uebersicht-Cyberangriffe-auf-kommunale-Verwaltungen-in-Deutschland-im-Jahr-2021.pdf.. Es wird kein Anspruch auf Vollständigkeit erhoben.

9 Bei der Einteilung wurde sich an der statistischen Einteilung von Städten orientiert, wobei nicht alle betroffenen Verwaltungen auch das Stadtrecht haben. Die folgenden statistischen Kategorien sind bei der Einteilung von Städten üblich: Landstädte = unter 5.000 Einwohner, Kleinstädte = 5.000–20.000 Einwohner, Mittelstädte = 20.000 bis 100.000 Einwohner, Großstädte = über 100.000 Einwohner (Schubert und Klein (2020)). Zusätzlich muss hier erwähnt werden, dass es sich im Falle von Anhalt-Bitterfeld sowie Ludwigslust-Parchim, um die Einwohnerzahl des Landkreises handelt.

10 Kommunalservice Mecklenburg (2021).

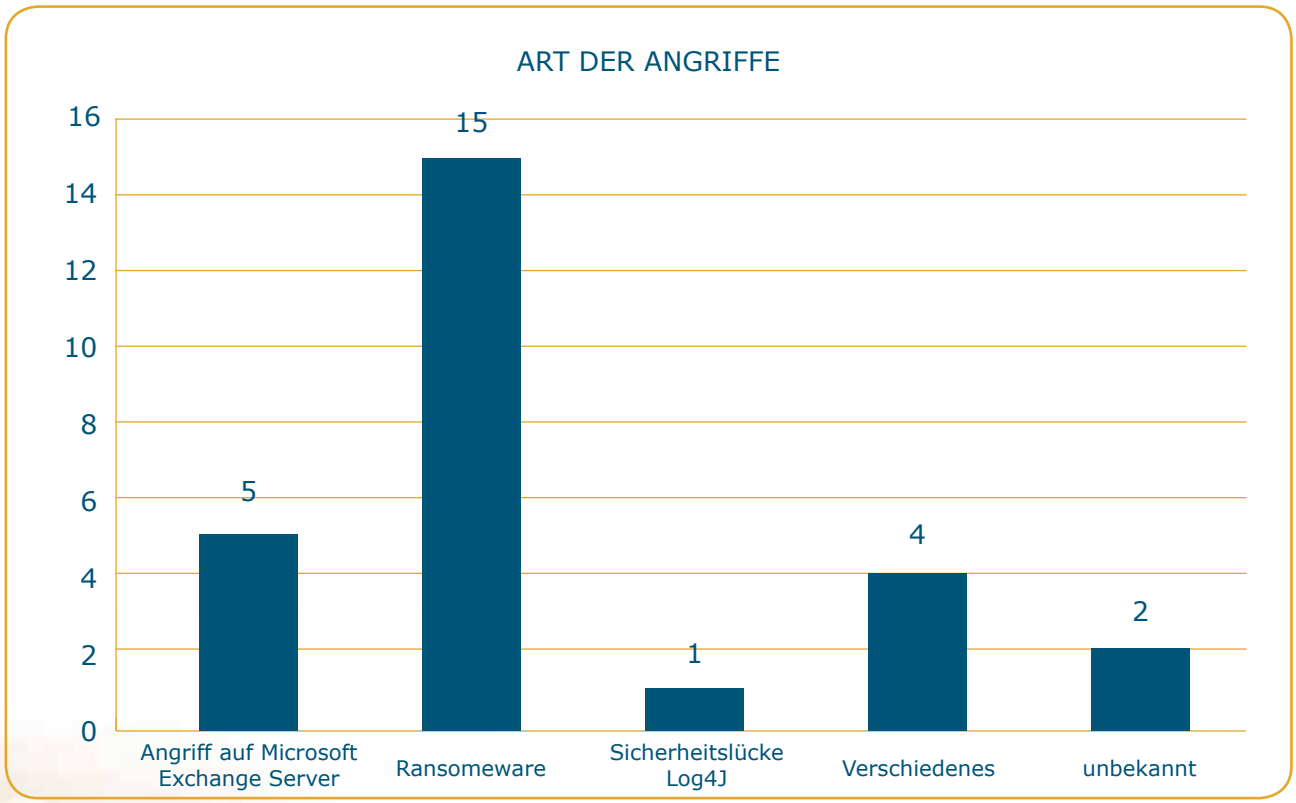
11 Hier muss erwähnt werden, dass aus den öffentlichen Informationen nicht eindeutig hervorging, welche weiteren Ämter über die Stadt Schwerin und den Landkreis Ludwigslust-Parchim betroffen waren. Aufgenommen wurden die Fälle, die verifiziert werden konnten durch Informationen auf den Seiten der betroffenen Ämter/Verwaltungen. Dies sind das Amt Grabow, das Amt Neustadt-Glewe, die Stadt Boizenburg/Elbe. Darüber hinaus hatten die Städte Greifswald und Stralsund auch mit Einschränkungen zu kämpfen. Mehr Informationen zu den einzelnen Fällen finden sich im Anhang der Studie unter: https://www.bigs-potsdam.org/app/uploads/2022/03/Uebersicht-Cyberangriffe-auf-kommunale-Verwaltungen-in-Deutschland-im-Jahr-2021.pdf.

12 Vgl. Bauer (2021); FRM Lokalpunktstudio (2021); Heinig (2021); MDR (2021).

13 Vgl. Stadt Bochum (2021).

Unter „Verschiedenes" wurden u.a. Angriffe gefasst, die nicht näher durch die entsprechenden Kommunen spezifiziert wurden, wie z. Bsp. ein Angriff auf ein E-Mail-Postfach. Abgegriffene Daten wurden dann wohl benutzt, um Phishing-E-Mails zu versenden, die den Eindruck vermitteln sollten, dass es sich um eine E-Mail eines Mitarbeiters der Stadtverwaltung Beverungen handle, eine Kommune in Nordrhein-Westfalen.[14] Im Fall von Witten, einer Stadt in Nordrhein-Westfalen, wurde nur von einem Ausfall der IT-Systeme gesprochen, dieser war jedoch beträchtlich.[15] Ein besonders dreister Fall ist der Hackerangriff auf das Rathaus in Rodenberg. Unbekannte griffen das Rathaus an, um die Rechenleistung der Computer für das Schürfen von Bitcoins zu verwenden.[16]

Abbildung 2: Art der Angriffe auf kommunale Verwaltungen in Deutschland 2021



Quelle: Eigene Darstellung.

Hafnium nutzte im Februar/März eine bis dahin nicht gepachte[18] Schwachstelle in Microsoft Exchange Server aus und unternahm einen weltweiten Exchange-Massenhack. Microsoft hatte zwar am 3. März 2021 außerplanmäßige Sicherheitsupdates zur Verfügung gestellt (ursprünglich war der 9. März als Patchday vorgesehen), doch es gab zum Teil auch Probleme beim Einspielen der Patches.[19] Das BSI ging alleine in Deutschland von zehntausenden betroffenen Exchange-Servern aus.[20]

In einem Fall gab es einen Zusammenhang mit dem Kaseya-Angriff im Juli 2021. Der Cyberangriff auf Lieferketten des US-amerikanischen Softwareunternehmens betraf ungefähr 1.500 Unternehmen, viele davon sogenannte Managed Service Providers, die

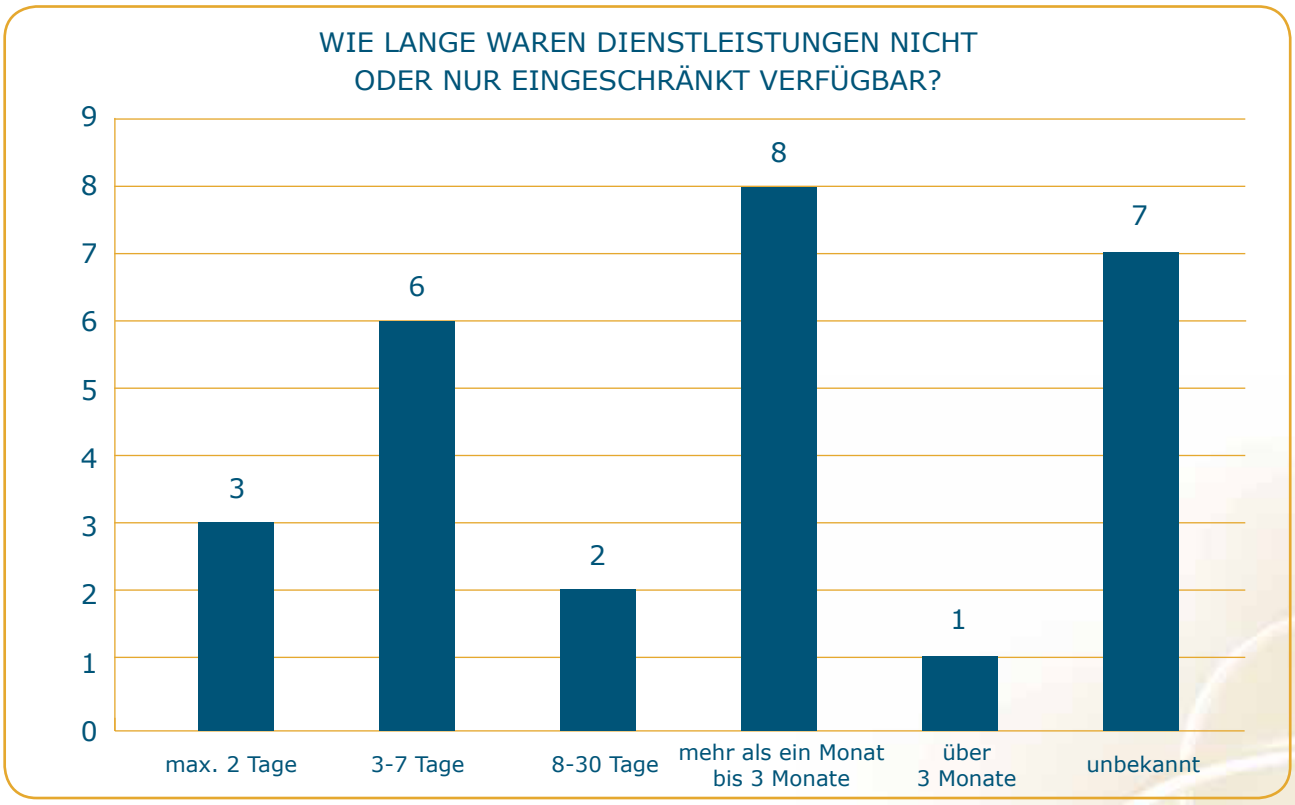
14 Vgl. Westfalen-Blatt (2021).
15 Vgl. Wilkens (2021).
16 Vgl. Schaumburger Nachrichten (2021).
17 Vgl. Bauer (2021); FRM Lokalpunktstudio (2021); Heinig (2021); MDR (2021).
18 Patchen bedeutet die Auslieferung einer Korrektur für die Behebung von Fehlern einer Software für den Endanwender. Meistens handelt sich es hierbei, um Sicherheitslücken oder die Nachrüstung von vorher nicht vorhandenen Funktionen.
19 Vgl. Born (2021).
20 Vgl. Bundesamt für Sicherheit in der Informationstechnik (o. J.).

Hauptkunden von Kaseya. Verantwortlich für den Angriff auf Kaseya war die in Russland ansässige Hackergruppe ReEvil.[21]

Im Fall von Anhalt-Bitterfeld scheint die seit Mai 2021 aktive Hackergruppe Grief hinter dem Angriff zu stecken. Diese agiert unter dem Namen „Pay or Grief". Wenn nicht gezahlt wird, tauchen oftmals abgegriffene Daten im Darknet auf, dies ist auch im Fall von Anhalt-Bitterfeld geschehen.[22]

Wie lange kommunale Verwaltungen durch einen Cyberangriff nicht oder nur bedingt handlungsfähig sind, ist abhängig von der Art des Cyberangriffes, welche Systeme zu welchem Grad betroffen sind, aber auch der Größe der Verwaltung. Hinzu kommt, dass es Verwaltungen, die sich auf das *Worst-Case-Szenario* „erfolgreicher Cyberangriff" vorbereitet haben, z. Bsp. durch Business *Continuity Management* Pläne oder durch das Vorhalten von Back-ups ein stückweit einfacher haben und möglicherweise auch schneller bei der Wiederherstellung der Systeme sind. Allerdings zeigt sich, dass eine Mehrheit der Kommunen – bei denen die Dauer der Einschränkungen bekannt waren – mit Ausfällen und Einschränkungen ihrer Dienstleistungen von über einer Woche oder deutlich länger zu kämpfen hatten.

Abbildung 3: Zeitraum, in dem Verwaltungen ihre Dienstleistungen nicht oder nur eingeschränkt anbieten konnten



Quelle: Eigene Darstellung.[23]

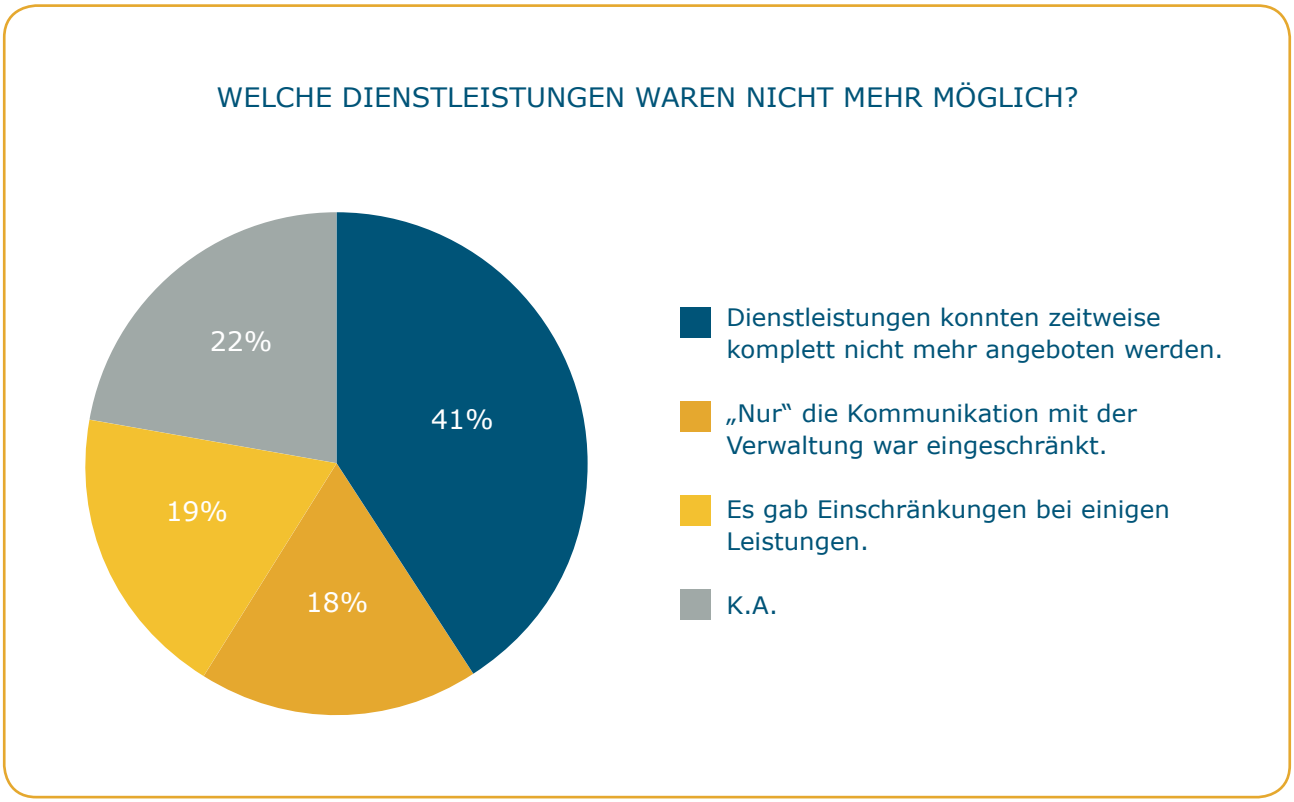
Während in manchen Fall wenigstens für einen gewissen Zeitraum keinerlei Dienstleistungen mehr möglich waren, gab es in anderen Verwaltungen „nur" Einschränkungen in der Kommunikation mit der Verwaltung (per Telefon und/oder E-Mail). In anderen Fällen waren wiederum nur einige Leistungen beschränkt. Welche dies genau waren, ist oftmals nicht im Detail bekannt.

21 Siehe für mehr Details auch Kern und Szanto (im Druck).

22 Vgl. Czerwonn (2021).

23 Der Stichtag zur Berechnung des Zeitraums war hierbei der 31.12.2021. Im neuen Jahr hatten insbesondere der Landkreis Ludwigslust-Parchim sowie die Verwaltung der Stadt Schwerin noch mit den Folgen des Cyberangriffes auf SIS und KSM zu kämpfen. Ludwigslust-Parchim wie Schwerin erklärten beide zum Zeitpunkt zur Verfassung dieser Analyse, dass sie einen stabilen Notbetrieb hergestellt haben, es aber noch dauern dürfte bis ein Normalbetrieb wieder möglich ist (Vgl. SIS - Schweriner IT- und Servicegesellschaft mbH (2021); SIS - Schweriner IT- und Servicegesellschaft mbH und Kommunalservice Mecklenburg (2021)).

Abbildung 4: Welche Dienstleistungen waren eingeschränkt?



Quelle: Eigene Darstellung.

In nur drei der 27 Fälle ist bekannt, dass Daten später entweder im Darknet aufgetaucht sind oder Daten von Dritten über ein E-Mailpostfach abgegriffen wurden wie im Fall der Stadt Beverungen.[24] In Anhalt-Bitterfeld wurden personenbezogene Daten von mindestens 92 Personen im Darknet veröffentlicht, 42 davon sind Mitglieder des Kreistages.[25] Im Fall der Stadt Witten wurden verschiedene Dokumente etwa ein Monat nach dem Vorfall im November 2021 gefunden. Dabei war alles von leeren Word-Vorlagen, zu Schriftverkehr mit der Stadt, aber in einigen Fällen auch Kopien von Reisepässen dabei.[26]

Eine weitere relativ unbekannte Größe ist die der durchschnittlichen Kosten für Kommunen nach einem erfolgreichen Cyberangriff. Zum Teil mag dies daran liegen, dass manche der Angriffe sich erst im 3. Quartal von 2021 ereignet haben und die Kommunen Anfang 2022 selber noch keinen Überblick hatten, wie hoch die Gesamtkosten sind. Oftmals wird dies allerdings auch nicht öffentlich kommuniziert. Bei 81% der vorliegenden Fälle liegen keine genaueren Informationen über die Kosten vor. In den fünf Fällen wo Kosteneinschätzungen vorliegen, vermelden Ebeleben und Wesel Kosten im niedrigen Bereich bei einer Summe bis 25.000€.[27] Im Fall von Geisenheim geht man von mindestens 180.000€ bis zu einem hohen fünfstelligen Betrag aus.[28] Im Fall von Angermünde sind die Kosten wohl im sechsstelligen Bereich angesiedelt.[29] In Anhalt-Bitterfeld geht der zuständige Landrat Grabner von Gesamtkosten von 1,7 bis zwei Millionen Euro aus. Allerdings steht ein abschließender Kassensturz noch aus und der Cyberangriff wird sich finanziell auch noch 2022 bemerkbar machen.[30] Diese Zahlen zeigen, dass es im Zweifel sehr teuer werden kann.

24 Vgl. Westfalen-Blatt (2021).
25 Vgl. Maxwill (2021).
26 Vgl. WDR (2021).
27 Vgl. Jessen (2021); MDR (2021).
28 Vgl. Pehl (2021).
29 Vgl. Matthies (2021).
30 Vgl. Ebert (2022).

EXKURS: DER ANGRIFF AUF ANHALT-BITTERFELD

Der Angriff auf den Landkreis Anhalt-Bitterfeld im Juli 2021 ist der wohl bekannteste und schwerwiegendste Cyberangriff auf eine kommunale Verwaltung Deutschlands im letzten Jahr. Am Morgen des 6. Juli wurde ein Mitarbeiter des Landkreises beim Hochfahren seines Computers mit der folgenden Nachricht begrüßt: *„Landkreis Anhalt-Bitterfeld, you are fucked. Do not touch anything"*.[31] Man geht inzwischen davon aus, dass die Angreifer schon zu Beginn des Jahres oder zumindest Wochen vor dem Angriff in den Systemen waren. Am 5. Juli wurden dann mit PowerShell[32] Befehlen Backdoors, also sogenannte Hintertüren, installiert, um so Zugang zum System zu erhalten. In der Nacht vom 5. auf den 6. Juli lief die Verschlüsselung der Systeme.[33]

In Anhalt-Bitterfeld führte der Ransomware-Angriff dazu, dass keine der 160 Fachanwendungen mehr funktionierte. Sozialleistungen und ähnliches konnten nicht mehr ausgezahlt werden. Alle Computer mussten heruntergefahren werden. Der Landkreis bekam von der Gruppe „Pay or Grief" eine 19-tägige Zahlungsfrist. Kurz vor Ende dieser Frist stellte die Gruppe erbeutete Daten ins Darknet.[34] Problematisch war, dass die Angreifer z. T. Logs gelöscht haben und Daten verschlüsselt wurden. Damit ist es schwieriger den Angriff nachzuvollziehen und welche Systeme sowie Endgeräte betroffen sind. Im Endeffekt musste Anhalt-Bitterfeld seine komplette IT von Grund auf neuaufbauen.[35] 80-90% der Daten konnten im Nachhinein dabei aus Backups wiederhergestellt werden.[36]

Der Angriff auf Anhalt-Bitterfeld ist bemerkenswert aufgrund von zwei Aspekten:

Zum ersten Mal wurde in einer Kommune nach einem Cyberangriff der Katastrophenfall ausgerufen. In aller Regel geschieht dies sonst nur aufgrund von Naturkatastrophen, um dadurch leichter die Unterstützung des Landes oder des Bundes zu erlangen. Hintergrund war insbesondere, dass viele finanzielle Belange von Bürgern und Bürgerinnen betroffen waren. Der Landkreis begründete die Entscheidung u.a. auch damit, dass Anhalt-Bitterfeld hierdurch schneller Entscheidungen selber treffen konnte.[37] Zudem hatte der Landkreis die Möglichkeit, schneller neue Hardware anzuschaffen, um so ein Notnetz aufzubauen, da man weniger stark an das strenge Vergaberecht gebunden ist. Auch weitere Hilfe von außen konnte hierdurch in Anspruch genommen werden.[38]

Dieser Einsatz von außen ist die zweite Besonderheit. Zum ersten Mal leistete das Kommando Cyber- und Informationsraum Amtshilfe nach einem Cyberangriff. Dabei waren bis zu sieben IT-Kräfte der Bundeswehr vom 3. bis zum 27. August in Anhalt-Bitterfeld vor Ort, um die IT-Infrastruktur sicher wiederaufzubauen.[39] Der Landkreis hatte u. a., um Amtshilfe ersucht, da Unterstützung bei der Forensik und beim Wiederaufbau benötigt wurde. Insbesondere ging es, um die Analyse und Wiederaufsetzung der über 900 Computer des Landkreises.[40] Dieser Einsatz wurde kritisch kommentiert und zur Kenntnis genommen. Problematisch ist ein stückweit, wieso bei einem Cyberangriff direkt Hilfe vonseiten des Bundes in Anspruch genommen werden muss und es nicht auch entsprechende zivile Einrichtungen auf Landesebene gibt, die sich zuerst der Sache annehmen.

Am 31.01.2022 erklärte Anhalt-Bitterfeld nach 206 Tagen den Katastrophenfall für beendet. In dieser Zeit wurde mühsam die IT-Infrastruktur wiederaufgebaut. Nicht alles lief zu dem Zeitpunkt wieder einwandfrei, aber der Zustand war soweit wiederhergestellt, sodass der Landkreis arbeitsfähig war.[41] Die Kosten dafür liegen bei etwa zwei Millionen Euro.[42]

31 Tremmel (2021).
32 PowerShell ist eine, von Microsoft entwickelte, objektorientierte Automatisierungs-Engine und Skriptsprache mit einer interaktiven Befehlszeile. PowerShell soll dabei u. a. bei der Konfiguration von Systemen wie auch bei der Automatisierung vom Verwaltungsaufgaben führen. Ein PowerShell Befehl führt dazu, dass eine Aktion durchgeführt wird. In diesem Fall die Installation der Backdoor und die anschließende Verschlüsselung des Systems.
33 Vgl. Tremmel (2021).
34 Vgl. Huesmann (2021).
35 Vgl. Tremmel (2021).
36 Vgl. Heinrich-Böll-Stiftung (o. J.).
37 Vgl. RND (2021).
38 Vgl. Tremmel (2021).
39 Vgl. Pump (2021).
40 Vgl. IT-Daily (2022).
41 Ibid.
42 Vgl. MDR (2022).

Laut Aussagen des zuständigen Landrats, Andy Grabner, hätte Anhalt-Bitterfeld besser aufgestellt sein können. Der Landkreis hätte mehr in IT-Sicherheit investieren müssen.[43] Das soll sich jetzt ändern, Anhalt-Bitterfeld will unter den Kommunen in Zukunft zum Vorreiter im Bereich IT-Sicherheit werden. Einiges hat sich seit dem Cyberangriff auch schon getan. So wird es in Anhalt-Bitterfeld zukünftiges ein eigenes IT-Amt geben in dem alle Personen, die mit der Administration von Rechnern beschäftigt sind, sitzen. Ein IT-Sicherheitsbeauftragter wird nicht mehr nur einfach ernannt, sondern durch ein Auswahlverfahren berufen und dafür speziell geschult. Die Vorgaben wie u. a. für Passwörter und Definitionen von Prozessen sind restriktiver als vor dem Angriff.[44]

DER BLICK INS AUSLAND

Cyberangriffe auf kommunale Verwaltungen sind bei weitem nicht nur ein deutsches Problem. Auch in anderen Teilen der Welt wurden Verwaltungen im Jahr 2021 Ziel von u.a. Ransomwarevorfällen, Datenklau und Phishing. Sei es in der australischen Stadt Stonnigton, in der Metropolregion Melbourne, wo ein Hackerangriff im August 2021 zu dem Ausfall von digitalen Leistungen und des ePlanning-Portals der Stadtverwaltung führte, welches offline genommen wurde.[45] Oder die tschechische Stadt Olomouc, wie auch die spanische Stadt Legunés, eine Vorstadt von Madrid, die beide Ziele von Angriffen wurden, die dazu führten, dass die Dienstleistungen der Städte stark eingeschränkt waren. Oder auch in Brasilien, wo im Bundestaat Santa Catarina die Webseiten von mindestens 245 der 295 Gemeinden des Bundesstaates zeitweise offline waren.[48]

Ransomware spielte ähnlich wie in Deutschland auch global eine große Rolle.

Insbesondere die Gruppe „Pay or Grief", die auch für den Vorfall in Anhalt-Bitterfeld verantwortlich ist, war im letzten Jahr aktiv. So erwischte es u.a. ebenfalls im Juli 2021 die französische Stadt Villepoint. Der Angriff im Juli 2021 verlief für die französische Stadt jedoch glimpflicher als für Anhalt-Bitterfeld. Lediglich die Kommunikation mit der Stadt per E-Mail und telefonisch war eingeschränkt. Weitere Informationen, wie detailliertere (technische) Angaben über den Angriff, die Kosten für die Stadt oder auch die Höhe der Lösegeldforderung sind nicht bekannt.[49] Weitere bekannte Fälle der Hackergruppe auf kommunale Verwaltungen sind die griechische Stadt Thessaloniki,[50] die italienische Gemeinde Comune di Porto Sant'Elpidio sowie die lokale Verwaltung von Mobile County, Alabama.[51]

Aber auch jenseits der Gruppe „Pay or Grief" wurden weitere kommunale Verwaltung Opfer von Ransomware-Angriffen. Die Schweregrade dabei sind oft unterschiedlich. Während manche über Wochen oder sogar Monate nur eingeschränkt handlungsfähig sind, verläuft es bei manchen glimpflicher. Auch wie kommunale Verwaltungen auf Ransomware-Angriffe reagieren ist sehr unterschiedlich. Allerdings ist es oft, dass wenig bis gar nichts an die Öffentlichkeit kommuniziert wird. In aller Regel scheint es so, dass die Kommunen Lösegeldforderungen nicht zahlen, aber auch hier gibt es Ausnahmen.

In Joplin, Missouri, wurde die kommunale Verwaltung im Juli 2021 Ziel eines Ransomware-Angriffs. In Fall von Joplin zahlte ein Versicherer $320,000 an eine unbekannte Person/Gruppe, damit keine sensiblen Daten veröffentlicht werden. Es ist nicht öffentlich bekannt, ob am Ende tatsächlich keine Daten im Darknet aufgetaucht sind oder über welche Daten, die Angreifer verfügten. Aufgrund des Ransomware-Angriffs waren die Onlineservices

43 Huesmann (2021).
44 Heinrich-Böll-Stiftung (o. J.).
45 Vgl. Hendry (2021).
46 Vgl. Idnes (2021).
47 Vgl. 20minutos (2021).
48 Vgl. Lobo (2021).
49 Vgl. Rieß-Marchive (2021).
50 Vgl. eKathimerini (2021).
51 Vgl. Paganini (2021).

Foto © Gorodenkoff / Shutterstock.com

von Joplin stark eingeschränkt. Die Stadt benötigte mehrere Wochen, um die IT-Infrastruktur wiederaufzubauen.[52]

Der Gemeindeverband Saint-Avold in Frankreich wurde auch Opfer eines Ransomware-Angriffes.Es war zeitweise nicht möglich, E-Mails zu senden oder zu empfangen und auf Akten, insbesondere Finanzakten, zuzugreifen. Saint-Avold verlor einiges an Daten, was insbesondere zu Schwierigkeiten bei der Arbeit am kürzlich verabschiedeten Haushalt sowie bei der Verwaltung der Gehälter von Mitarbeitenden führte. Es wurde die Summe von $80,000 gefordert, um wieder Zugang zu verlorenen Daten zu erlangen. Die Stadt entschied sich jedoch dagegen das „Lösegeld" zu zahlen und baute die IT-Infrastruktur eigenständig wieder auf.[53]

Aufmerksamkeit erregte der Ransomware-Angriff auf die nordschwedische Gemeinde Kalix im Dezember 2021. Im Gegensatz zu vielen anderen Opfern von Ransomware, kommunizierte Kalix transparent über den Angriff. Dies wurde auch von der EU-Kommissarin für Inneres, Ylva Johansson, gelobt.[54] Die Gemeinde entschied sich dagegen zu zahlen. In Schweden haben wohl bereits „zwei Drittel aller 290 Gemeinden Erfahrung gemacht mit Erpressungssoftware, die ihnen mehr oder weniger schadete."[55]

Wie man es nicht machen sollte, zeigt der Fall der schweizerischen Gemeinde Rolle. Der Angriff im Mai 2021 wurde von dem Nachrichtenportal watson im August 2021 publik gemacht. Die Gemeinde bestätigte erst nach mehrfacher Nachfrage den Angriff. In dieser ersten Bestätigung sprach die Bürgermeisterin der Gemeinde noch davon, dass angeblich keine sensiblen Daten gestohlen wurden.[56]

Doch nicht nur war die Kommunikation intransparent, sondern dies war offensichtlich auch falsch und die Gemeinde war zudem wohl auch nachlässig bei der Aufarbeitung. So gelangten hochsensible Daten von etwa 5.500 Einwohnern und Einwohnerinnen (u. a. Name, Geburtsdatum, Steuernummer,

52 Vgl. Woodin (2021).
53 Vgl. Louis (2021).
54 Vgl. Selnes (2021).
55 Meissl Årebo (2022).
56 Vgl. Schurter und Wietlisbach (2021).

Kreditdaten) der Gemeinde, von Angestellten wie auch Unternehmen ins Darknet.[57] Doch als die Gemeinde Ende Juni mitbekam, dass gestohlene Daten im Darknet aufgetaucht waren, wurden keine Sofortmaßnahmen getroffen und dies nicht in die Breite kommuniziert. Noch im August war der Zugriff auf mindestens zwei externe Datenbanken durch entsprechende Links und Passwörter in den veröffentlichten Dateien möglich. Das lässt vermuten, dass die E-Mails nicht entsprechend gescannt wurden, um solche mit Zugangsdaten zu erkennen, um dann die Zugänge zu widerrufen.[58]

Neben Ransomware, spielte weltweit auch insbesondere Phishing eine größere Rolle. Teilweise waren die Kommunen selber Opfer von Phishing-Angriffen, aber teilweise wurden auch E-Mail-Zugänge von kommunalen Verwaltungen verwendet, um Phishing-Emails zu versenden.

So wurde im Dezember 2021 in der US-amerikanischen Kleinstadt Colchester, Vermont, der E-Mailzugang der Stadt verwendet, um betrügerische E-Mails zu versenden. Geklärt ist noch nicht, ob dies aufgrund eines Virus geschehen ist oder ob Angreifer Zugriff auf die Emailkonten der Stadt hatten.[59] Ein ähnlicher Fall ereignete sich im Oktober 2021 in der Schweizer Gemeinde Mellingen. Der Zugriff auf die E-Mail-Konten der Gemeinde wurde genutzt, um Spam-Mails an verschiedene Adressaten zu verschicken, welche Malware enthielt.[60]

LeClarire, Iowa, war von November 2020 bis Februar 2021 das Ziel von Phishing. Durch täuschend echt wirkende E-Mails von drei Dienstleistern der Stadt wurden insgesamt $222,373 auf falsche Konten überwiesen. Der Stadt gelang es zum Teil das Geld wieder zu bekommen.[61]

Die Beispiele hier zeigen vermutlich nur einen Bruchteil der Cyberangriffe mit denen sich kommunale Verwaltungen in anderen Teilen der Welt im Jahr 2021 auseinandersetzen mussten. Viele sind womöglich öffentlich nicht bekannt, werden verschwiegen oder sind noch nicht aufgefallen. Die Kommunikation über Cyberangriffe ist auch weltweit weitestgehend intransparent. Doch bei den hier zusammengetragenen Fällen, lässt sich ein ähnliches Muster wie in Deutschland erkennen: Auch in anderen Ländern sind kommunale Verwaltungen insbesondere mit Ransomware-Angriffen konfrontiert. Es zeigt sich, dass kommunale Verwaltungen global vor ähnlichen Herausforderungen stehen.[62]

57 Vgl. Computerworld (2021).
58 Vgl. Anz (2021).
59 Vgl. Office of the Vermont Attorney General (2022).
60 Vgl. Elber (2021).
61 Vgl. Watson (2021).
62 Einen Überblick über weitere Cyberangriffe auf kommunale Verwaltungen weltweit findet sich online auf der Webseite des BIGS: https://www.bigs-potsdam.org/app/uploads/2022/03/Uebersicht-Cyberangriffe-auf-kommunale-Verwaltungen-weltweit-im-Jahr-2021.pdf. Dabei wird kein Anspruch auf Vollständigkeit erhoben.

HANDLUNGSEMPFEHLUNGEN

Wenn Cyberangriffe auf Kommunen glimpflich ablaufen, mögen vielleicht nur einige wenige Leistungen eingeschränkt sein und nach ein paar Tagen kann die Kommune wieder normal agieren. In anderen Fällen kann es jedoch Wochen oder Monate dauern, bis die Leistungen für die Menschen wieder verfügbar sind. Neben den Kosten, die auf Kommunen zusätzlich zukommen, ist der potenzielle Vertrauensverlust von Menschen in staatliche (demokratische) Strukturen besonders schwerwiegend. Dieses Vertrauen muss erst wieder mühsam zurückgewonnen werden.

Weiterhin sind Kommunen die staatlichen Organe, die finanzielle Hilfen wie Sozialleistungen auszahlen. Hier hat der Staat eine Fürsorgefunktion. Wenn er dieser Funktion, sei es auch nur für einen kurzen Zeitraum für eine kleine Gruppe nicht nachkommen kann, ist dies problematisch.

Kommunalen Verwaltungen sind zudem diejenigen, die die meisten Schnittstellen zu Bürgerinnen und Bürgern haben und auch über entsprechende Daten verfügen. Bei Angriffen mit Ransomware kommt es immer wieder vor, dass Daten als Druckmittel eingesetzt werden, um doch noch an Geld zu kommen, wenn die betroffenen Kommunen nicht zahlen. Teilweise werden als Folge auch sensible Daten im Darknet veröffentlicht, wenn die Erpressungssumme nicht gezahlt wird. Zudem können Zugänge zu E-Mailkonten genutzt werden, um Phishing-Mails zu versenden.

Wie die genaue Bedrohungslage für kommunale Verwaltungen aussieht, ist schwierig einzuschätzen. Die öffentliche Datenlage kann nur als mangelhaft bezeichnet werden. Aber auch die nichtöffentliche Datenlage scheint nicht viel besser zu sein. Einer Umfrage von Zeit Online und des Bayrischen Rundfunks unter allen Bundesländern zum Thema Ransomware ergab, dass einige Bundesländer nicht einmal erfassen wie viele Angriffe es mit Ransomware auf staatliche Strukturen innerhalb ihres Gebiets gibt, wie dies z. Bsp. In Nordrhein-Westfalen oder Berlin der Fall ist. Andere Länder wie Thüringen erfassen Daten erst seit 2019.

Gleichzeitig stellt Ransomware nur einen Teil der Problematik mit Cyberangriffen dar, wenn auch einen vergleichsweise großen. Sofern die Länder jedoch nicht selber tätig werden, müssen die betroffenen Kommunen niemanden einen Cyberangriff melden, außer sie stellen Strafanzeige bei der zuständigen Strafverfolgungsbehörde. Nur die Bundesbehörden müssen Ransomware-Angriffe gegenüber dem BSI kundgeben. Hier liegen dem BSI laut eigener Aussage keine Meldungen vor.[63]

Doch aufgrund dieser Datenlücke ist auch nicht klar, wie sich das Problem entwickelt. Wird es zu einem immer größeren Problem, weil Kommunen mehr und mehr Dienstleistungen digitalisieren und gleichzeitig die Bedrohungslage insgesamt steigt? Oder werden Kommunen im Laufe der Zeit besser darin diese Angriffe abzuwehren, weil sie sich entsprechend besser aufstellen und schützen?

Eine Einschätzung ist weitestgehend unmöglich zu geben, da es an belastbaren Zahlen fehlt. Natürlich zeigt die allgemeine Bedrohungslage, dass in der nächsten Zeit das Problem sehr wahrscheinlich erst einmal größer wird als kleiner. Die Zahl von Angriffen mit Ransomware wächst, gleichzeitig ist es heute durch Ransomware-as-a-Service Angeboten (RaaS) auch für Menschen ohne großes technisches Wissen relativ einfach sich entsprechende Dienste einzukaufen.

Neben der Entwicklung und dem Einsatz der Schadsoftwarevariante kann z. Bsp. ein 24/7 Support, weitere gebündelte Angebote, aber auch Funktionen, die von legitimen Software-as-a-Service (SaaS) angeboten werden, dazu gekauft werden. Die Kosten hierfür sind im Vergleich zu den potenziellen Gewinnen vergleichsweise gering. Laut einer Studie von Crowdstrike lag die durchschnittliche Lösegeldforderung bei $6 Millionen im Jahr 2021. Die Preise von RaaS fangen aktuell bei etwa $40 im Monat an, können aber auch bis zu mehreren Tausend Dollar betragen.[64]

Doch es fehlt nicht nur an der Datenlage, wie oft kommunale Verwaltungen von Cyberangriffen be-

63 Vgl. Biermann (2021).
64 Vgl. Baker (2022).

Foto © bluebay / 123RF.com

troffen sind, wie hoch die Kosten hierfür sind, sondern auch weitestgehend wie Kommunen im Bereich IT-Sicherheit überhaupt aufgestellt sind. Zu vermuten ist eine relativ heterogene Infrastruktur mit Kommunen, die große Lücken aufweisen und solchen, die im Vergleich schon relativ gut aufgestellt sind. Dies bedeutet aber auch, dass nicht so einfach evaluiert und validiert werden kann, welche Maßnahmen erfolgreich sind, um Kommunen resilienter aufzustellen. Oder auch welche Maßnahmen dazu geführt haben, dass die Kosten für Kommunen nicht exorbitant hoch sind, wenn sie z. Bsp. ihre komplette IT-Infrastruktur wiederherstellen müssen.

Die Intransparenz zu Cyberangriffen auf kommunale Verwaltungen erschwert zudem auch das Teilen von Informationen, *Lessons Learnt* und *Best Practices* unter den Kommunen. Wenn man nicht weiß, dass ein Angriff stattgefunden hat, kann man auch bei der entsprechenden Kommune nicht nachfragen.

Zudem heißt dies auch, dass das Lernen und die Lehren aus solchen Angriffen sich auf einige spektakuläre Angriffe wie der Fall von Anhalt-Bitterfeld konzentriert. Es benötigt also Möglichkeiten für Kommunen sich einfach und relativ unbürokratisch über Cyberangriffe, *Best-Practices* und Entwicklungen der Bedrohungslage auszutauschen sowie auch sensible Daten miteinander zu teilen.

Immer wieder sprechen Kommunen im Falle eines Cyberangriffes von einem Gefühl erst einmal ziemlich alleine mit dem Problem da zu stehen. Dies steht erst einmal im Widerspruch, wenn man sich die staatliche Cybersicherheitsarchitektur in Deutschland, aufbereitet durch die Stiftung Neue

Verantwortung, anschaut.[65] An entsprechenden Akteuren im Cybersicherheitsbereich scheint es nicht zu mangeln. Jedoch führt diese Fülle an Akteuren auch zu einer Unübersichtlichkeit und Informationsflut. Wer für was und wen zuständig ist, ist kaum noch zu überblicken.

Die wenigsten Kommunen haben vermutlich sofort den richtigen Ansprechpartner parat, wenn sie mit einem Cybervorfall zu kämpfen haben. Abhilfe schaffen würde in diesem Fall eine stärkere Vernetzung der Kommunen untereinander, aber auch mit den auf Länderebenen angesiedelten Einrichtungen. Zudem ist es so, dass das BSI für die Kommunen nicht zuständig ist, sondern nur für den Bund. D. h. wenn es nicht entsprechende Organisationen auf Länderebene gibt, die auch für die Kommunen zuständig sind, gibt es niemanden, der sich explizit, um die Belange der kommunalen Verwaltungen kümmert.

Zu der Komplexität der vorhandenen Akteure, kommt eine Informationsflut im Bereich Cybersicherheit. Insbesondere für kleine kommunale Verwaltungen, deren IT-Team aus maximal zwei bis drei Personen besteht, besteht kaum die Möglichkeit, sich rechtzeitig und effizient über Risiken sowie aktuelle Entwicklungen zu informieren. Solche kleinen Teams sind in aller Regel schon damit ausgelastet die normale IT am Laufen zu halten. Jedoch können solche Informationen Verwaltungen vor erfolgreichen Cyberangriffen bewahren, in dem sie aufgrund dieser Kenntnisse rechtzeitig Updates einspielen, bekannte Sicherheitslücken durch Patches schließen sowie Mitarbeitende auf Risiken hinwiesen wie z. Bsp. laufende Phishingkampagnen.

Nordrhein-Westfalen ist hier vorangegangen und hat einen neuen kommunalen Warn- und Informationsdienst gegründet, der die Kommunen über IT-Sicherheitshinweise informiert, die auch die Landesverwaltung erhält. Zudem soll so auch die Kooperation zwischen Land und Kommunen im Bereich IT-Sicherheit verstärkt werden.[66] Aber es bleibt abzuwarten, ob dieses Angebot von den Kommunen angenommen wird und ob es nicht zu einer Erhöhung der Informationsflut führt.

Kommunen müssen sich verstärkt mit den Cybersicherheitsrisiken auch für kommunale Verwaltungsinfrastruktur auseinandersetzen. Daran führt in Zeiten vermehrter Digitalisierung und steigender Abhängigkeit von IT kein Weg vorbei, auch auf kommunaler Ebene, während das Risiko wächst.

Die meisten Angriffe verlaufen nach dem *low-hanging fruit* Prinzip. Angriffe werden breit gestreut und vorhandene Schwachstellen ausgenutzt. Die Organisationen, ohne oder nur mit niedrigen Cybersicherheitsstandards sind dann gefundene Opfer, da der Einsatz für die kriminellen Akteure niedrig bleibt, bei potenziell größeren Summen, die erpresst oder Daten, die im Darknet verkauft werden können. Kommunen sollten daher mindestens versuchen, den BSI IT-Grundschutz umsetzen. Hierfür gibt es auch ein entsprechendes Profil für die Kommunalverwaltung, welches von der Arbeitsgruppe „Modernisierung IT-Grundschutz" mit Unterstützung des Deutscher Städtetags, des Deutschen Landkreistags und des Deutschen Städte- und Gemeindebund erarbeitet wurde.[67]

Zudem braucht es *Business Continuity Pläne* bzw. Notfallpläne für den Fall eines erfolgreichen Cyberangriffes. D. h. es sollte im Vorfeld geklärt werden, wer für was zuständig ist, an welche Ansprechpartner man sich im Notfall wenden kann und welche Maßnahmen ergriffen werden muss. Ein zu bildender Krisenstab kann helfen, um Maßnahmen und Verantwortlichkeiten zu koordinieren.

Die Erstellung eines solchen Planes kann zudem helfen, kritische Schwach- und Schnittstellen im Vorhinein zu erkennen und dort ggf. weitere Sicherheitsmaßnahmen umzusetzen. Präventive Maßnahmen, wie das Vorhalten von Backups, können aus solchen Plänen abgeleitet werden. Darüber hinaus braucht es gerade aber auch Wiederherstellungskonzepte, um so die Dienstleistungen von Verwaltungen so schnell wie möglich wieder anzubieten. Denn ein einfaches Backup reicht nicht, wenn es über 100 verschiedene Fachanwendungen gibt, deren Systeme historisch gewachsen sind.[68] Außerdem müssen Backups natürlich so gestaltet werden, dass sie im Notfall überhaupt eingesetzt werden können. Wenn

65 Vgl. Herpig und Rupp (2021).
66 Vgl. Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen (2022).
67 Vgl. Bundesamt für Sicherheit in der Informationstechnik et al. (2019).
68 Vgl. Tremmel (2021).

die Backups auch verschlüsselt oder kompromittiert wurden, hilft auch das Backup nicht weiter.

Auch das einmalige Aufstellen eines solchen Plans reicht nicht aus, sondern dieser muss auch gelebt werden. Dies bedeutet die regelmäßige Überprüfung und etwaige Aktualisierung, aber auch Notfallübungen wie Schreibtischübungen oder Penetrationstests zur Überprüfung der Netzwerksicherheit.

Das auch Verwaltungen Opfer von Cyberangriffen werden ist nicht weiter verwunderlich. Eine vollständige Sicherheit kann und wird es nicht geben. Allerdings können trotzdem die Hürden für Angreife erhöht werden durch präventive Maßnahmen in die Resilienz der IT-Systeme. Außerdem können Notfallkonzepte erstellt werden, um den Schaden nach einem erfolgreichen Angriff so klein wie möglich und die Kosten so niedrig wie möglich zu halten sowie die Dauer des Ausfalls von Verwaltungsdienstleistungen zu verringern.

Staat und Verwaltung gehören zu den kritischen Infrastrukturen, aufgrund der Tatsache, dass „eine Störung oder gar ein Ausfall einzelner Einrichtungen [sich] negativ auf die öffentliche Ordnung auswirken [kann]. Insbesondere ein Ausfall von Behörden im Bereich der Gefahrenabwehr kann für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung folgenschwere Konsequenzen haben."[69] Doch im Gegensatz zu anderen KRITIS-Bereichen gibt es keine klaren Kriterien, welche Kommunen KRITIS sind und welche vielleicht aufgrund ihrer Größe oder potenzieller Ausweichstandorte möglicherweise nicht. Darüber hinaus bedeutet dies auch, dass die Pflichten für Kommunen nicht genauer definiert sind. Notwendig wäre es zudem eine systematische Übersicht über kommunale Dienstleistungen zu erstellen und diese Leistungen zu priorisieren. Dies ist auch hilfreich bei der Erstellung von Wiederanlaufplänen. Hier gilt es insgesamt auch gesetzgeberisch nachzuschärfen, umso die IT-Sicherheit deutschlandweit auf kommunaler Ebene zu stärken und resilienter zu gestalten.

69 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (o. J.).

Literaturangaben

20minutos (2021). Un ataque informático tumba el sistema del Ayuntamiento de Leganés. https://www.20minutos.es/noticia/4918269/0/ataque-informatico-ayuntamiento-leganes/?autoref=true (zuletzt abgerufen: 21.03.2022).

Anz, P. (2021). Cyberangriff auf Rolle: Es wird noch schlimmer. Inside IT. https://www.inside-it.ch/post/cyberangriff-auf-rolle-es-wird-noch-schlimmer-20210830 (zuletzt abgerufen: 21.03.2022).

Baker, K. (2022). Ransomware as a Service (RaaS) Explained. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (zuletzt abgerufen: 21.03.2022).

Bauer, N. (2021). Dreiste Hackerangriffe aus China: Gemeinden aus Freising werden zum Opfer Krimineller. Merkur. https://www.merkur.de/lokales/freising/freising-ort28692/fahrenzhausen-ort88182/freising-gemeinden-werden-opfer-von-hackerangriffen-aus-china-90260836.html (zuletzt abgerufen: 21.03.2022).

Biermann, K. (2021). Der Staat als Beute. Die Zeit. https://www.zeit.de/digital/datenschutz/2021-06/erpressung-internet-kommunen-behoerden-oeffentliche-einrichtungen-ransomware-attacken/komplettansicht (zuletzt abgerufen: 21.03.2022).

Biselli, A. (2020). Cyberhilfswerk: Sandsäcke stapeln im Internet. Golem. https://www.golem.de/news/cyberhilfswerk-sandsaecke-stapeln-im-internet-2005-147781.html (zuletzt abgerufen: 21.03.2022).

Born, G. (2021). Der Hafnium Exchange-Server-Hack: Anatomie einer Katastrophe. Heise. https://www.heise.de/news/Der-Hafnium-Exchange-Server-Hack-Anatomie-einer-Katastrophe-5077269.html (zuletzt abgerufen: 21.03.2022).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (o. J.). Staat und Verwaltung. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/Staat-Verwaltung/staat-verwaltung_node.html (zuletzt abgerufen: 21.03.2022).

Bundesamt für Sicherheit in der Informationstechnik. (o. J.). Kritische Schwachstellen in Exchange-Servern. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Server/Microsoft-Exchange_Schwachstelle/schwachstelle_exchange_server_node.html (zuletzt abgerufen: 21.03.2022).

Bundesamt für Sicherheit in der Informationstechnik. (2021). Die Lage der IT-Sicherheit in Deutschland 2021.

Bundesamt für Sicherheit in der Informationstechnik, Deutscher Städtetag, Deutscher Landkreistag & Deutscher Städte- und Gemeindebund. (2019). IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung.

Computerworld (2021). Gemeinde Rolle räumt Fehler im Umgang mit Cyberangriff ein. https://www.computerworld.ch/security/hacking/gemeinde-rolle-raeumt-fehler-im-umgang-cyberangriff-2692682.html?ganzseitig=1 (zuletzt abgerufen: 21.03.2022).

Czerwonn, F. (2021). Nach Cyberangriff auf Anhalt-Bitterfeld: Spekulationen um Name der Hackergruppe - „Pay or Grief" soll hinter Lösegeldforderung stecken. Mitteldeutsche Zeitung. https://www.mz.de/lokal/bitterfeld/spekulationen-um-name-der-hackergruppe-pay-or-grief-soll-hinter-losegeldforderung-stecken-3222917 (zuletzt abgerufen: 21.03.2022).

Ebert, K. (2022). Alles wird teurer: Folgen des Cyberangriffs kosten Landkreis Anhalt-Bitterfeld bis zu zwei Millionen. Mitteldeutsche Zeitung. https://www.mz.de/lokal/koethen/alles-wird-teurer-folgen-des-cyberangriffs-kosten-landkreis-anhalt-bitterfeld-bis-zu-zwei-millionen-3322297 (zuletzt abgerufen: 21.03.2022).

eKathimerini (2021). Thessaloniki Municipality shuts down after hack. https://www.ekathimerini.com/news/1165098/thessaloniki-municipality-shuts-down-after-hack/ (zuletzt abgerufen: 21.03.2022).

Elber, C. (2021). Nach Mellingen: So gefährlich sind Hackerangriffe auf Gemeinden. Aargauer Zeitung. https://www.aargauerzeitung.ch/aargau/diebe-aus-dem-homeoffice-so-gefaehrlich-sind-hackerangriffe-auf-gemeinden-ld.2216582 (zuletzt abgerufen: 21.03.2022).

FRM Lokalpunktstudio (2021). Rathausschließung am 16.04.2021 und 19.04.2021. https://frm.lokal.studio/2021/04/08/rathausschliessung-am-16-04-2021-und-19-04-2021/ (zuletzt abgerufen: 21.03.2022).

Grüner, S. (2021). Staatsanwaltschaft ermittelt nach IT-Angriff auf Schwerin. Golem. https://www.golem.de/news/ransomware-staatsanwaltschaft-ermittelt-nach-it-angriff-auf-schwerin-2111-161294.html (zuletzt abgerufen: 21.03.2022).

Heinig, C. (2021). Hacker dringen in E-Mail-Server der Gemeinde Schöneiche ein. MOZ. https://www.moz.de/lokales/erkner/cyberangriff-hacker-dringen-in-e-mail-server-der-gemeinde-schoeneiche-ein-55874866.html (zuletzt abgerufen: 21.03.2022).

Heinrich-Böll-Stiftung. (o. J.). Cyberangriff auf Landkreis Anhalt-Bitterfeld 2021. https://kommunalwiki.boell.de/index.php/Cyberangriff_auf_Landkreis_Anhalt-Bitterfeld_2021 (zuletzt abgerufen: 21.03.2022).

Hendry, J. (2021). Melbourne's Stonnington council hit by suspected cyber attack. iTnews. https://www.itnews.com.au/news/melbournes-stonnington-council-hit-by-suspected-cyber-attack-569283 (zuletzt abgerufen: 21.03.2022).

Herpig, S. & Rupp, C. (2021). Deutschlands staatliche Cybersicherheitsarchitektur.

Huesmann, F. (2021). Die Katastrophe aus dem Netz – wie digitale Lösegelderpresser eine Kreisverwaltung lahmlegten, RND. https://www.rnd.de/politik/digitalisierte-katastrophe-wie-hacker-eine-kreisverwaltung-lahmlegten-QMGICDPU2NG67CTETDPZDBPGSA.html (zuletzt abgerufen: 21.03.2022).

Idnes (2021). Olomoucký magistrát paralyzoval útok hackerů, město podá trestní oznámení. https://www.idnes.cz/olomouc/zpravy/olomouc-magistrat-utok-hackeru-datova-sit-kolaps.A210407_175516_olomouc-zpravy_stk (zuletzt abgerufen: 21.03.2022).

IT-Daily (2022). Trojaner legt Landratsamt lahm: Behörde geht von Hackerangriff aus. https://www.it-daily.net/shortnews/29438-trojaner-legt-landratsamt-lahm-behoerde-geht-von-hackerangriff-aus (zuletzt abgerufen: 21.03.2022).

Jessen, J. (2021). Cyberangriff auf Kreisverwaltung Wesel – Hintergründe unklar. NRZ. https://www.nrz.de/region/niederrhein/cyberangriff-die-kreisverwaltung-wesel-id233630387.html (zuletzt abgerufen: 21.03.2022).

Kern, E. & Szanto, A. (im Druck). Cyber Supply Chain Attacks (BIGS Policy Paper Nr. 9).

Kommunalservice Mecklenburg. (2021). Krisenbewältigung nach Cyberangriff. https://www.ks-mecklenburg.de/.content/nachricht/nachricht_00080.html (zuletzt abgerufen: 21.03.2022).

Lobo, A. P. (2021). Ataque hacker tira do ar sites de 245 prefeituras de Santa Catarina. Convergencia. https://www.convergenciadigital.com.br/Seguranca/Ataque-hacker-tira-do-ar-sites-de-245-prefeituras-de-Santa-Catarina-58909.html (zuletzt abgerufen: 21.03.2022).

Louis, J.-M. (2021). Cyberattaque: la communauté d'agglomération Saint-Avold Synergie victime d'une tentative de rançon. La Semaine. https://www.lasemaine.fr/cyberattaque-la-communaute-dagglomeration-saint-avold-synergie-victime-dune-tentative-de-rancon/ (zuletzt abgerufen: 21.03.2022).

Matthies, J. (2021). Kosten bei Hacker-Angriff könnten für die Uckermark sechsstellig sein. https://www.moz.de/lokales/schwedt/digitalisierung-sicherheit-uckermark-kosten-bei-hacker-angriff-koennten-fuer-die-uckermark-sechsstellig-sein-57623053.html (zuletzt abgerufen: 21.03.2022).

Maxwill, P. (2021). Hacker stellen persönliche Daten von Abgeordneten ins Darknet. Der Spiegel. https://www.spiegel.de/netzwelt/netzpolitik/anhalt-bitterfeld-hacker-stellen-persoenliche-daten-von-abgeordneten-ins-darknet-a-b3655f6d-0002-0001-0000-000178686047 (zuletzt abgerufen: 21.03.2022).

MDR (2021). Online-Erpresser verschlüsseln Behörden-Computer in Ebeleben. https://www.mdr.de/nachrichten/thueringen/nord-thueringen/kyffhaeuser/ebeleben-hackerangriff-digitale-erpressung-trojaner-100.html (zuletzt abgerufen: 21.03.2022).

MDR (2022). Anhalt-Bitterfeld will Vorreiter bei Cyber-Sicherheit werden. https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/bitterfeld/landkreis-vorreiter-cybersicherheit-100~amp.html (zuletzt abgerufen: 21.03.2022).

Meissl Årebo, I. (2022). «Wir lassen uns nicht erpressen»: Eine schwedische Gemeinde geht nach einem Cyberangriff an die Öffentlichkeit. Neue Zürcher Zeitung. https://www.nzz.ch/international/hackerangriff-schwedische-gemeinde-geht-an-die-oeffentlichkeit-ld.1669101 (zuletzt abgerufen: 21.03.2022).

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen. (2022). Nordrhein-Westfalen stärkt Cybersicherheit in den Kommunen mit neuem Warn- und Informationsdienst. https://www.wirtschaft.nrw/pressemitteilung/nordrhein-westfalen-staerkt-cybersicherheit-den-kommunen-mit-neuem-warn-und (zuletzt abgerufen: 21.03.2022).

Nationaler Normenkontrollrat. (2021). Monitor Digitale Verwaltung #6.

NDR (2021). Cyberangriff in Westmecklenburg: Kein Normalbetrieb mehr in diesem Jahr. https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Cyberangriff-in-Westmecklenburg-Kein-Normalbetrieb-mehr-in-diesem-Jahr,itausfall114.html (zuletzt abgerufen: 21.03.2022).

Office of the Vermont Attorney General. (2022). Town of Colchester Data Breach Notice to Consumers. https://ago.vermont.gov/blog/2022/01/19/town-of-colchester-data-breach-notice-to-consumers/ (zuletzt abgerufen: 21.03.2022).

Paganini, P. (2021). Prometheus and Grief – two new emerging ransomware gangs targeting enterprises. https://securityaffairs.co/wordpress/118446/cyber-crime/prometheus-grief-ransomware.html (zuletzt abgerufen: 21.03.2022).

Pehl, P. (2021). Interview mit Christian Aßmann und Linus Neumann. Podcast. In Cyberangriff auf die Stadtkasse – Wie erlebt das ein Bürgermeister? Kommunal. https://kommunal.de/cyberangriff-stadtkasse-buergermeiseter-berichtet (zuletzt abgerufen: 21.03.2022).

Pump, M. (2021). Amtshilfe in Bitterfeld - IT-Informationstechnik-Soldaten im zivilen Einsatz. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/amtshilfe-in-bitterfeld-5217614 (zuletzt abgerufen: 21.03.2022).

Rieß-Marchive, V. (2021). Cyberattaque: la ville de Villepinte confrontée au ransomware Grief, LeMagIT. https://www.lemagit.fr/actualites/252503487/Cyberattaque-la-ville-de-Villepinte-confrontee-au-ransomware-Grief (zuletzt abgerufen: 21.03.2022).

RND (2021). Katastrophenfall nach Cyberattacke im Landkreis Anhalt-Bitterfeld. https://www.rnd.de/panorama/hackerangriff-in-anhalt-bitterfeld-katastrophenfall-landkreisverwaltung-weiterhin-nicht-U5BPUQHAIO5QXGMHSFCKUY6U44.html (zuletzt abgerufen: 21.03.2022).

Schaumburger Nachrichten (2021). Unbekannte starten Hackerangriff auf das Rodenberger Rathaus um Bitcoin zu schürfen. https://www.sn-online.de/Schaumburg/Rodenberg/Samtgemeinde-Rodenberg/Rodenberg-Unbekannte-starten-Hackerangriff-auf-Rathaus-fuer-Bitcoin (zuletzt abgerufen: 21.03.2022).

Schubert, K. & Klein, M. (2020). Stadt. In K. Schubert & M. Klein (Hrsg.), Das Politiklexikon (7. Aufl.). Bundeszentrale für Politische Bildung.

Schurter, D. & Wietlisbach, O. (2021). Schweizer Gemeinde wird gehackt und verschweigt Datendiebstahl – Leak im Darknet. watson. https://www.watson.ch/digital/schweiz/987644812-hacker-veroeffentlichen-gb-an-vertraulichen-daten-der-gemeinde-rolle-vd (zuletzt abgerufen: 21.03.2022).

Selnes, A. (2021). Kalix får EU-beröm efter it-attack. Europaportalen. https://www.europaportalen.se/2021/12/kalix-far-berom-av-eu-efter-it-attack (zuletzt abgerufen: 21.03.2022).

SIS - Schweriner IT- und Servicegesellschaft mbH. (2021). Nach Cyberangriff - auf dem Weg zum stabilen IT-Notbetrieb. https://www.sis-schwerin.de/.content/nachricht/nachricht_00054.html (zuletzt abgerufen: 21.03.2022).

Literaturangaben

SIS - Schweriner IT- und Servicegesellschaft mbH; Kommunalservice Mecklenburg. (2021, 17. Dezember). Presseupdate KW 50 [Pressemitteilung]. https://www.kreis-lup.de/output/download.php?fid=3378.4186.1.PDF (zuletzt abgerufen: 21.03.2022).

Stadt Bochum. (2021, 20. Dezember). IT-Sicherheitslücke: Services der Stadt übergangsweise nicht erreichbar [Pressemitteilung]. https://www.bochum.de/Pressemeldungen/20-Dezember-2021/IT-Sicherheitsluecke-Services-der-Stadt-uebergangsweise-nicht-erreichbar (zuletzt abgerufen: 21.03.2022).

Tremmel, M. (2021). Rebuilding Landkreis Anhalt-Bitterfeld. Golem. https://www.golem.de/news/nach-ransomware-katastrophe-rebuilding-landkreis-anhalt-bitterfeld-2112-162045.html (zuletzt abgerufen: 21.03.2022).

Watson, S. (2021). City of LeClaire paid $222,373 to email scammers posing as vendors. The Gazette. https://www.thegazette.com/local-government/city-of-leclaire-paid-222373-to-email-scammers-posing-as-vendors/ (zuletzt abgerufen: 21.03.2022).

WDR (2021). Nach Hackerangriff: Stadt Witten wurden doch Daten gestohlen. https://www1.wdr.de/nachrichten/ruhrgebiet/stadt-witten-hacker-haben-daten-geklaut-100.html (zuletzt abgerufen: 21.03.2022).

Westfalen-Blatt (2021). Hackerangriff in der Beverunger Stadtverwaltung. https://www.westfalen-blatt.de/owl/kreis-hoexter/beverungen/hackerangriff-in-der-beverunger-stadtverwaltung-1066077 (zuletzt abgerufen: 21.03.2022).

Wilkens, A. (2021). Cyberangriff: Stadtverwaltung Witten online nicht erreichbar. Heise. https://www.heise.de/news/Cyberangriff-Stadtverwaltung-Witten-online-nicht-erreichbar-6221937.html (zuletzt abgerufen: 21.03.2022).

Woodin, D. (2021). Ransomware Shuts Down Online Services in Joplin, Mo. Government Technology. https://www.govtech.com/security/ransomware-shuts-down-online-services-in-joplin-mo (zuletzt abgerufen: 21.03.2022).

Die Zeit (2021). Cyberangriff mit Schadsoftware „DeepBlueMagic". https://www.zeit.de/news/2021-11/22/cyberangriff-mit-schadsoftware-deepbluemagic (zuletzt abgerufen: 21.03.2022).

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Geschäftsführender Direktor:
Dr. Tim H. Stuchtey
Dianastraße 46 · 14482 Potsdam
info@bigs-potsdam.org
www.bigs-potsdam.org

IMPRESSUM

Das BIGS (Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH) ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes wissenschaftliches Institut, das zu gesellschaftswissenschaftlichen Fragen ziviler Sicherheit forscht. Das Institut publiziert seine Forschungsergebnisse und vermittelt diese in Veranstaltungen an eine interessierte Öffentlichkeit. Das BIGS entstand im Frühjahr 2010 in Potsdam unter der Beteiligung der Universität Potsdam und ihrer UP Transfer GmbH sowie der Unternehmen IABG, Rolls-Royce und seit 2018 W.I.S.. Alle Aussagen und Meinungsäußerungen in diesem Papier liegen in der alleinigen Verantwortung der Autorin.

Autorin:
Esther Kern

Titel:
Cyberangriffe auf deutsche Kommunen im Jahr 2021

Herausgeber:
Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH

Verantwortlicher im Sinne des Rundfunkstaatsvertrages:
Dr. Tim H. Stuchtey

ISSN 2191-6756

Weitere Informationen über die Veröffentlichungen des BIGS befinden sich auf der Webseite des Instituts:

www.bigs-potsdam.org

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT