HAGEN
Stadt der FernUniversität
Der Oberbürgermeister



**Drucksachennummer:**
0041/2021

**Datum:**
15.01.2021

# ÖFFENTLICHER VORSCHLAG ZUR TAGESORDNUNG

**Absender:**
SPD-Fraktion im Rat der Stadt Hagen

**Betreff:**
Vorschlag der SPD-Fraktion
hier: Mögliche Hackerangriffe auf die Hagener Stadtverwaltung

**Beratungsfolge:**
04.02.2021 Haupt- und Finanzausschuss

**Beschlussvorschlag:**
In Anbetracht des Hackerangriffs auf die Funke-Mediengruppe, deren Auswirkungen für mehrere Wochen auch in den Hagener Medien zu spüren waren, berichtet die Verwaltung über eigene Erfahrungen mit der immer stärker um sich greifenden Cyber-Kriminalität und erläutert, welche Maßnahmen zur IT-Sicherheit in der Stadtverwaltung und den städtischen Beteiligungen bereits getroffen werden. Welche Abwehrstrategien sind darüber hinaus geplant und gibt es dafür Unterstützung von Land und/oder dem Bund?

Nach dem Bericht der Verwaltung behält sich die SPD-Ratsfraktion vor, Anträge zum Thema zu stellen.

**Kurzfassung**

entfällt

**Begründung**

siehe Anlage

## Inklusion von Menschen mit Behinderung

Belange von Menschen mit Behinderung

[X] sind nicht betroffen

## Auswirkungen auf den Klimaschutz und die Klimafolgenanpassung

[ ] keine Auswirkungen (o)

SPD-Fraktion
im Rat der Stadt Hagen

Rathausstraße 11-13 Postfach 42 49
58095 Hagen 58042 Hagen
spd-fraktion-hagen@online.de

02331 207 - 3505
02331 207 - 2495
www.spd-hagen.de

Herrn
Oberbürgermeister
Erik O. Schulz
im Hause

Hagen, 14. Januar 2021

**Möglicher Hackerangriffe auf die Hagener Stadtverwaltung**

Sehr geehrter Herr Oberbürgermeister Schulz,

wir bitten um Aufnahme des og. Antrages für die nächste Sitzung des Haupt- und Finanzausschusses gem. § 6 Abs.1 GeschO, am 04. Februar 2021.

**Beschlussvorschlag:**

In Anbetracht des Hackerangriffs auf die Funke-Mediengruppe, deren Auswirkungen für mehre Wochen auch in den Hagener Medien zu spüren waren, berichtet die Verwaltung über eigene Erfahrungen mit der immer stärker um sich greifenden Cyber-Kriminalität und erläutert, welche Maßnahmen zur IT-Sicherheit in der Stadtverwaltung und den städtischen Beteiligungen bereits getroffen werden. Welche Abwehrstrategien sind darüber hinaus geplant und gibt es dafür Unterstützung von Land und/oder dem Bund?

**Begründung:**

Dass kriminelle Hacker immer wieder versuchen, auf Daten von Unternehmen zuzugreifen, um letztendlich Geld zu erpressen, ist seit geraumer Zeit aus den Medien hinlänglich bekannt. Welche gravierenden Auswirkungen ein solcher Angriff aber haben kann, das wurde auch uns hier in Hagen mit dem jüngsten Angriff auf das Computersystem der Funke-Mediengruppe und damit auf die Westfalenpost und den Stadtanzeiger vor Augen geführt. Tag für Tag berichteten die betroffenen und damit technisch lahm gelegten lokalen und überregionalen Redaktionen über die enormen Schwierigkeiten, um die IT-Systeme nach dem Cyber-Angriff wiederinstandsetzen und aktivieren zu können.

Auch musste sich das Unternehmen von Kunden und Lesern fragen lassen, ob die ihm übermittelten privaten Daten (Adresse, Konto, Telefon, E-Mail, etc.) nunmehr den kriminellen Angreifern in die Hände gefallen sind. Neben dem enormen wirtschaftlichen Schaden ist hier auch ein Imageschaden entstanden.

Es ist daher zu vermuten, dass öffentliche Verwaltungen und ihre Beteiligungen, die nicht zuletzt für die Daseinsvorsorge zuständig sind, ebenfalls ins Fadenkreuz dieser Art von Kriminalität rücken. Wie die Fachzeitschrift „Kommune 21“ in ihrer neuesten Ausgabe berichtet, gründet das Land Baden-Württemberg eigens eine Cyber-Sicherheitsagentur (s. Anlage 1), um bei der Abwehr von Internet-Kriminalität schlagfertiger zu werden. Unterstützt werden sollen dabei auch die Kommunen im Land.
Im Nachbarland Bayern greift das Landesamt für Sicherheit in der Informationstechnik den Kommunen bei der Abwehr von Cyber-Angriffen unter die Arme (s. Anlage 2).
Die Begründung: „Die Umsetzung von IT-Sicherheit ist eine wachsende und fachliche komplexe Aufgabe, welche die Kommunen vor immer größere Herausforderungen stellt.“

Nach dem Bericht der Verwaltung behält sich die SPD-Ratsfraktion vor, Anträge zum Thema zu stellen.

Freundliche Grüße

Claus Rudel
SPD-Ratsfraktion

Anlage IT-Sicherheit 1.pdf

Anlage IT-Sicherheit 2.pdf

# Angriffen **Paroli bieten**

Thomas Strobl

**Baden-Württemberg will bei der Abwehr von Internet-Kriminalität schlagkräftiger werden und gründet dazu eine eigene Cyber-Sicherheitsagentur. Diese soll künftig als zentrale Koordinierungs- und Meldestelle fungieren.**

Ob Mitteldeutscher Rundfunk, die Uniklinik Düsseldorf, das Robert-Koch-Institut, Handwerkskammern oder Industrieunternehmen – sie alle wurden bereits Opfer von Cyber-Angriffen. In einer Umfrage des Branchenverbands Bitkom gaben drei Viertel aller befragten Unternehmen an, Ziel von Cyber-Kriminalität geworden zu sein. Auch Verwaltungen und Behörden, Forschungseinrichtungen oder Einzelpersonen geraten in den Fokus von Cyber-Kriminellen. Die Schäden gehen allein wirtschaftlich betrachtet in die Milliarden.

Menschen, Institutionen und Unternehmen im digitalen Raum bestmöglich zu schützen, ist Aufgabe der Politik. In Baden-Württemberg trägt das Ministerium für Inneres, Digitalisierung und Migration daher nicht nur für die klassischen Themen der inneren Sicherheit wie Polizei und Bevölkerungsschutz Verantwortung, sondern auch für die Cyber-Sicherheit. Eine größtmögliche Sicherheit in diesem Bereich ist ein entscheidender Faktor für die nachhaltige Entwicklung und Wettbewerbsfähigkeit und somit auch ein wichtiger Standortfaktor. Denn Baden-Württemberg ist ohne Zweifel ein lukratives Ziel für Cyber-Kriminelle. Die vielen erfolgreichen Unternehmen im Land, Forschungseinrichtungen, aber auch Verwaltungen und öffentliche Einrichtungen stehen im Fokus. Bei den Angriffen geht es um ganz unterschiedliche Dinge: den Diebstahl von Wissen und Know-how, Angriffe aus finanziellen Motiven oder auf sensible Infrastrukturen.

Baden-Württemberg hat das erkannt und setzt entsprechende Maßnahmen um. Dazu gehört unter anderem die Gründung einer eigenen Cyber-Sicherheitsagentur. Sie wird das Herz der neuen Cyber-Sicherheitsinfrastruktur sein und soll potenziellen Angriffen auf die digitalen Infrastrukturen Paroli bieten. Im September 2020 hat das Kabinett den Entwurf für das „Gesetz zur Verbesserung der Cyber-Sicherheit" verabschiedet, der die Cyber-Sicherheitsagentur auf den Weg bringt.

Es folgten Wochen im Oktober und November mit viel Lesestoff, denn im Rahmen der Verbandsanhörung und eines Bürgerbeteiligungsverfahrens gingen zahlreiche Stellungnahmen ein. Die Auswertung dieser Meinungen und Anregungen ergab: Ein großer Teil der eingebrachten Impulse bewertet das Vorhaben positiv. Mit den Kritikpunkten haben sich die Verantwortlichen auseinandergesetzt und an der ein oder anderen Stelle den Gesetzestext nachjustiert. Wichtig ist es dem Land, alle Beteiligten früh einzubeziehen und gemeinsam mit den anderen Akteuren im Bereich der Cyber-Sicherheit zusammenzuarbeiten. Um schlagkräftiger zu werden, soll die bisher dezentral organisierte Abwehr von Gefahren aus dem Internet besser vernetzt werden. Bisher müssen noch alle öffentlichen Stellen im Land eigene Strukturen schaffen und die erforderlichen technischen Voraussetzungen aufbauen.

**Hintergrund:**

Die Digitalisierung ist ein zentraler Arbeitsschwerpunkt der Landesregierung Baden-Württemberg. Mit digital@bw wurde im Sommer 2017 die erste landesweite und ressortübergreifende Digitalisierungsstrategie vorgestellt, die in Team-Arbeit von allen Ministerien erstellt wurde. Aktuell werden über 70 konkrete Projekte umgesetzt. Als eine der zentralen Voraussetzungen für die Digitalisierung hat die Landesregierung von Beginn an die Cyber-Sicherheit in ihre ressortübergreifende Digitalisierungsstrategie aufgenommen.
• www.digital-bw.de





Baden-Württemberg nimmt Cyber-Sicherheit in den Fokus.

Für die neue Cyber-Sicherheitsarchitektur stellt das Land Baden-Württemberg im Staatshaushalt 2020/2021 Mittel in Höhe von 13 Millionen Euro zur Verfügung. Innerhalb dieses finanziellen Rahmens hat der Gesetzgeber insgesamt 83 Stellen für die neu gegründete Agentur genehmigt. Von den 32 Stellen, die bereits seit Anfang 2020 zur Verfügung stehen, waren trotz der pandemiebedingten schwierigen Rahmenbedingungen Stand Anfang Dezember 2020 bereits 22 besetzt.

Die Cyber-Sicherheitsagentur soll künftig die zentrale Koordinierungs- und Meldestelle sein. In dieser Funktion sammelt sie Daten zur aktuellen Sicherheitslage und zu Angriffsszenarien im Land, dokumentiert diese und wertet sie aus. Anhand der gesammelten Daten soll ein landesweites Lagebild erstellt werden, das die Agentur zielgruppenorientiert weitergibt, gegebenenfalls durch Warnungen ergänzt und so das Niveau der Cyber-Sicherheit im Land erhöht. Außerdem soll die neue Institution Bürger, Wirtschaft, Wissenschaft und Verwaltung zum Thema Internet-Sicherheit sensibilisieren und beraten. Sie kann beispielsweise Kommunen dabei helfen, Schäden durch Cyber-Angriffe zu verhindern, sodass Verwaltungen im Falle eines Angriffs nicht komplett lahmgelegt werden. Das beginnt bei Workshops für die Mitarbeiter, geht über Schulungen für die IT-Administration bis hin zu konkreten Hinweisen auf Bedrohungs- und Gefährdungslagen. Alle Angebote haben letzten Endes das selbe Ziel: die IT-Infrastruktur des Landes und sensible Daten zu schützen. Doch auch, wenn es zu einem Angriff kam, kann die Cyber-Sicherheitsagentur unterstützen: Auf Ersuchen der betroffenen Stelle kann sie Maßnahmen treffen, die zur Wiederherstellung der Sicherheit und Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.

Das Kabinett hat das Gesetz im Dezember zur Behandlung in den Landtag eingebracht. Der Aufbaustab der neuen Landesoberbehörde soll – wenn alles nach Plan verläuft – im Frühjahr 2021 seine Arbeit aufnehmen. Dabei gilt es zunächst, Strukturen und Prozesse zu schaffen, die den operativen Betrieb ermöglichen. Die entsprechenden Vorbereitungen dafür laufen zum Teil schon jetzt. Zunächst wird sich die Agentur mit ihren Angeboten auf die Landesverwaltung und die Kommunen konzentrieren. Perspektivisch werden auch die Bürger, die Wirtschaft und die Wissenschaft einbezogen.

Dass für ein sicheres und selbstbestimmtes Handeln in einer zunehmend digitalisierten Umgebung ein gesamtgesellschaftlicher Ansatz erforderlich ist, hat bereits die Cyber-Sicherheitsstrategie der Bundesregierung aus dem Jahr 2016 festgestellt. Bedeutsam ist deshalb vor allem die Zusammenarbeit der Cyber-Sicherheitsagentur mit anderen Sicherheitsbehörden, also den regionalen Polizeipräsidien, dem Landeskriminalamt und dem Landesamt für Verfassungsschutz. Diese sind weiterhin gemäß ihrem gesetzlichen Auftrag in der Ermittlung und Prävention von Cyber-Attacken aktiv. Betroffenen wird nahegelegt, immer auch Anzeige zu erstatten und im Falle eines erpresserischen Angriffs kein Lösegeld zu bezahlen.

Besonders wichtig ist bei alldem der Faktor Mensch. Denn nur wer weiß, wo die Gefahren lauern und wie Angreifer agieren, kann sich wirksam schützen. Der Staat muss Sicherheit, Recht und Freiheit in unserem Land auch im digitalen Raum optimal gewährleisten. Hierzu bedarf es einer zeitgemäßen Cyber-Sicherheitsarchitektur, die die verschiedenen Akteure wirksam verzahnt. Nur mit einem ganzheitlichen Ansatz können die aktuellen und künftigen Herausforderungen, Bedrohungs- und Gefährdungslagen effektiv und effizient bewältigt werden.

*Thomas Strobl ist stellvertretender Ministerpräsident und Minister für Inneres, Digitalisierung und Migration Baden-Württemberg.*

# Umfassende **Unterstützung**

Daniel Kleffel

**In Bayern hilft das Landesamt für Sicherheit in der Informationstechnik den Kommunen dabei, sich gegen Cyber-Angriffe zu wappnen. Zum Angebot zählen unter anderem das Siegel „Kommunale IT-Sicherheit“ und Online-Kurse zur Sensibilisierung der Mitarbeiter.**

Als IT-Sicherheitsbehörde des Freistaats Bayern ist das Landesamt für Sicherheit in der Informationstechnik (LSI) unter anderem verantwortlich für den Schutz des Bayerischen Behördennetzes (BYBN) und die Beobachtung der Sicherheitslage. Die IT-Sicherheitsexperten des LSI verfügen somit über einen reichen Erfahrungsschatz bei der Detektion von Angriffen und der Nachverfolgung von möglichen IT-Sicherheitsvorfällen. Ebenso kennt das LSI aus der eigenen praktischen Arbeit und der engen Vernetzung, zum Beispiel im Verwaltungs-CERT-Verbund von Bund und Ländern, die jeweils aktuellen Hauptangriffsvektoren und deren Bedeutung speziell für die Verwaltung.

„Unser Landesamt für Sicherheit in der Informationstechnik ist ein Anker der IT-Sicherheit in Bayern. Bürger und Unternehmen müssen darauf vertrauen können, dass ihre Daten bei der Verwaltung gut und sicher aufgehoben sind“, fasst Bayerns Finanz- und Heimatminister Albert Füracker die Aufgabe des Amtes zusammen. Seit der Gründung zählt die Unterstützung und Beratung der 2.056 Kommunen im Freistaat zu einem der wichtigsten Tätigkeitsschwerpunkte des LSI. Der überwiegende Teil der Kommunen hat nur wenige tausend Einwohner und entsprechend kleine Verwaltungen. Die Umsetzung von IT-Sicherheit ist eine wachsende und fachlich komplexe Aufgabe, welche die Kommunen vor immer größere Herausforderungen stellt. Die täglichen Meldungen verdeutlichen, dass die Bedrohung keine Ausnahmen kennt. Kleine Gemeinden dürfen sich nicht darauf verlassen, dass ihre vermeintlich mangelnde Attraktivität sie vor Cyber-Angriffen schützt. Gleichzeitig stellt gerade der Einstieg in das Thema IT-Sicherheit für kleine Organisationen eine hohe Hürde dar.

Neumarkt i.d.Oberpfalz lässt IT-Sicherheit zertifizieren.*

Maßnahmen zur Verbesserung der kommunalen IT-Sicherheit müssen sich an den praktischen Bedürfnissen orientieren und vor Ort verfügbar gemacht werden. An dieser Stelle setzt die IT-Sicherheitsbehörde mit diversen Angeboten an. So geben die IT-Sicherheitsexperten der Behörde eigenes praktisches Wissen beispielsweise über Individualberatungen an die kommunale Ebene weiter. Kommunen erhalten vom LSI zudem aktuelle Informationen zur IT-Sicherheitslage und Warnmeldungen. Diese Angebote werden immer stärker nachgefragt. Im Jahr 2020 häuften sich aufgrund der Pandemielage insbesondere Beratungsanfragen zur sicheren Umsetzung von Telearbeit.

* v.l.: Werner Brandenburger, Vorsitzender der Verwaltungsgemeinschaft Neumarkt i.d.Oberpfalz und 1. Bürgermeister der Gemeinde Sengenthal; Rudolf Ehrensberger, IT-Systemadministrator der VG Neumarkt i.d.Oberpfalz; Bayerns Finanz- und Heimatminister Albert Füracker; Thomas Meier, 1. Bürgermeister der Gemeinde Berngau; LSI-Präsident Daniel Kleffel; Andreas Truber, 1. Bürgermeister der Gemeinde Pilsach





Ein zentraler Baustein für die IT-Sicherheit ist die Sensibilisierung der Mitarbeiter. Deshalb bietet das LSI allen bayerischen Kommunen einen kostenlosen Zugang zu Online-Kursen an, mit denen das Verwaltungspersonal regelmäßig hinsichtlich IT-Awareness geschult werden kann.

Im Dialog mit den Kommunen ist zudem das Siegel „Kommunale IT-Sicherheit“ entstanden. Dieses wurde auf Grundlage gängiger Informationssicherheits-Management-Systeme (ISMS) entwickelt. Der im Sommer 2019 veröffentlichte Maßnahmenkatalog des Siegels mit 47 Maßnahmen und dazugehörigen Prüffragen ist als eine Art Vorstufe zu einer Zertifizierung auf Basis einer Selbstauskunft zu sehen. Das Siegel gibt gerade kleineren Kommunen Orientierung und Unterstützung bei der gesetzeskonformen Einführung eines Informationssicherheitskonzepts nach Art. 11 Abs. 1 BayEGovG. Dabei berücksichtigt es vor allem Aspekte, die für die IT-Sicherheit kleinerer Kommunen eine übergeordnete Rolle spielen und bildet die zentralen Punkte aus den Bereichen IT-Sicherheitstechnik, interne Organisation und Mitarbeitersensibilisierung ab. 139 bayerische Kommunen haben mittlerweile das LSI-Siegel erhalten, das bis zu zwei Jahre gültig ist. Sollte eine Kommune bereits nach einem ISMS-Standard – etwa nach ISIS12 auf der Grundlage eines Förderprogramms des Bayerischen Innenministeriums – zertifiziert sein, kann im Falle einer Vergleichbarkeit die Zertifizierung anerkannt werden, um das Siegel „Kommunale IT-Sicherheit“ des LSI zu erhalten.

Ein neuer Baustein des LSI-Beratungsangebots für Kommunen sind Hilfestellungen im Bereich Notfall-Management. Denn auch kleine Städte und Gemeinden müssen sich mit der Frage beschäftigen, wie mit einem etwaigen Sicherheitsvorfall konkret umzugehen ist. Im Rahmen einer aktuellen Handreichung gibt das LSI hier praxisnahe Anregungen, unter anderem in Form von Hilfsmitteln, Dokumenten und einem Fragenkatalog. Es wird dabei ein Handlungsrahmen mit Regelungen zum Ausrufen eines Notfalls, Alarmierungsplänen, Notbetrieb, Wiederanlauf und Nacharbeit bei einem IT-Notfall geschaffen. Darüber hinaus sind Vorlagen für ein Notfallhandbuch, eine Notfallkarte, einen Vorsorgekalender, eine Notfall-Checkliste und Pressemitteilungen enthalten.

Die Beratungs- und Unterstützungsangebote des LSI wurden in enger Abstimmung mit den Kommunen entwickelt. So sind Konzepte entstanden, die sich an den tatsächlichen Bedürfnissen der kommunalen IT orientieren und gerade kleine Gemeinden zielgerichtet in den wirklich entscheidenden Fragen weiterbringen.

*Daniel Kleffel ist Präsident des Landesamts für Sicherheit in der Informationstechnik Bayern.*

**Link-Tipp**

Weitere Informationen zum Beratungsangebot des LSI sind zu finden unter:

- **www.lsi.bayern.de**