Landtag Mecklenburg-Vorpommern
8. Wahlperiode
**- Ausschuss für Inneres,
Bau und Digitalisierung -**

Ausschussdrucksache 8/55

Schwerin, den 25. März 2022

Schriftliche Stellungnahmen

zum Antrag der Fraktion der FDP
Cyberkriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen
- Drucksache 8/249 -

1. Landkreistag Mecklenburg-Vorpommern e. V.
2. Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
3. Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
4. Amt für Digitalisierung und IT Rostock
5. Schweriner IT- und Servicegesellschaft GmbH
6. Landesgeschäftsstelle des Bundes Deutscher Kriminalbeamter
7. Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Landkreistag Mecklenburg-Vorpommern

Geschäftsführendes Vorstandsmitglied

Landkreistag Mecklenburg-Vorpommern, Bertha-von-Suttner-Str. 5, 19061 Schwerin

Landtag Mecklenburg-Vorpommern
Ausschuss für Inneres, Bau und
Digitalisierung
Der Vorsitzende
Herr Abgeordneter Ralf Mucha
Lennéstr. 1 (Schloss)
19053 Schwerin

E-Mail: innenausschuss@landtag-mv.de

Haus der Kommunalen Selbstverwaltung
Bertha-von-Suttner –Straße 5
19061 Schwerin

Ihr Ansprechpartner:
Dr. Jonathan Fahlbusch
Telefon: (03 85) 30 31-311
E-Mail:
Jonathan.Fahlbusch@landkreistag-mv.de

Unser Zeichen: 062.11-Fa/Th
Schwerin, den 22. März 2022

Cyberkriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen
Stellungnahme des Landkreistages Mecklenburg-Vorpommern

Sehr geehrter Herr Vorsitzender Mucha,

der Ausschuss für Inneres, Bau und Digitalisierung des Landtages Mecklenburg-Vorpommern beabsichtigt, zum Antrag der Fraktion der FDP – „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen“ am 31. März 2022 eine öffentliche Anhörung durchzuführen. Ich danke Ihnen für die Gelegenheit, an der Anhörung teilzunehmen und hierzu schriftlich Stellung zu nehmen.

In der Anhörung wird Herr Dr. Jonathan Fahlbusch für den Landkreistag das Meinungsbild aus den Landkreisen darstellen, die sich aus der Arbeitsgruppe Information und Kommunikation (AG IuK) speist, die sich im Landkreistag u.a. um die Belange der IT-Sicherheit kümmert. In der AG IuK sind die Landkreise, die kreisfreien Städte, der Zweckverband Elektronische Verwaltung (eGo-MV), die Kommunalservice Mecklenburg (KSM AöR) und die IKT-Ost AöR (Innovation, Kommunikation, Tranformation) sowie die Fachhochschule Güstrow vertreten.

Stellungnahme:

Das Thema Informationssicherheit ist bei den Landkreisen seit den Sicherheitsvorfällen bei KSM, Stadt Schwerin und im Kreis Ludwigslust-Parchim tief ins Bewusstsein gerückt. Die Anforderungen aus dem Bereich der Digitalisierung an die öffentliche Verwaltung sind immens gestiegen und steigen mit der Umsetzung des Onlinezugangsgesetzes noch weiter an. Weiterer Treiber ist die im Zuge der Corona Pandemie gestiegene Erwartung an die Digitalisierung von Verwaltungsvorgängen. Durch die Digitalisierung und die Technisierung von Verwaltungsvorgängen wird die Verwaltung immer stärker abhängig von der Funktionalität und Verlässlichkeit der IT-Infrastrukturen und deren sicheren Betrieb.

Die Landkreise nehmen die IT-Sicherheit sehr ernst und haben IT-Sicherheitsbeauftragte ernannt.

Sie fahren derzeit unterschiedliche Strategien mit der Bündelung des Betriebs wie z.B. bei der KSM (LUP) bzw. der IKT Ost (MSE & VG) oder der Beauftragung eines externen Dienstleisters (wie z.B. in NWM) oder durch einen eigenständigen IT-Bereich innerhalb des Landkreises (wie z.B. in LRO & VR).

Ein gutes Sicherheitsniveaus ist nicht nur durch technische Standards und Strukturen zu gewährleisten, sondern setzt in hohem Maße den Einsatz professioneller personeller Ressourcen voraus. Dem Hinweis im Antrag der FDP-Fraktion, dass es einer besseren personellen Ausstattung für den Bereich IT-Sicherheit bedarf, ist aus Sicht der Landkreise zuzustimmen. Für die bessere personalwirtschaftliche Ausstattung der Landkreise sind jedoch zwei Voraussetzungen maßgeblich, die in der aktuellen Arbeitsmarktlage nicht ausreichend gegeben sind: Es bedarf einer ausreichenden Anzahl von Fachkräften, die in der öffentlichen Verwaltung für diese Aufgabe gewonnen werden kann und entsprechend ihrer Qualifikation vergütet wird. Zum zweiten bedarf es der Verbesserung von Kenntnissen und der Sensibilität für IT-Sicherheitsfragen auf Seiten der Beschäftigten innerhalb der öffentlichen Verwaltung. Das letztere Defizit bekämpfen die Landkreise mit Fortbildungen, Schulungen Dienstanweisungen, Appellen und Werbung. Wünschenswert ist aber auch die Vermittlung von mehr technischem Wissen und Verständnis in der Grundausbildung. Die rasante technische Entwicklung fordert hier alle heraus.

Abgesehen von den Schwierigkeiten, die am Fachkräftemarkt aktuell bestehen und die nur durch hohe Investitionen in die Ausbildungen an den Hochschulen aber auch in der regulären Verwaltungsfachausbildung gemindert werden können, bedarf es bei den Landkreisen neben den Investitionen in Personal auch solche in Infrastrukturen. Ein hohes IT-Sicherheitsniveau wird perspektivisch nicht ohne zusätzliche finanzielle Mittel zu stemmen sein, die die Landkreise nicht allein werden aufbringen können.

Die Herstellung einer IT-Sicherheitsstruktur muss über alle staatlichen Ebenen hinweg gedacht und gemeinsam von allen Gebietskörperschaften hergestellt werden. Denn die Digitalisierung bringt es mit sich, dass die Daten zwischen den Gebietskörperschaften und Behörden des Landes, der Landkreise und der Gemeinden, den Bürgerinnen und Bürgern sowie Unternehmen hin und her fließen, und deshalb Zugriffe illegaler Art an einer beliebigen Stelle des gemeinsamen Netzes eine Gefahr für alle im Netz angeschlossenen Stellen nach sich zieht. Auch dies ist eine Lehre aus dem Sicherheitsvorfall in SN/LUP.

Die Landkreise sehen deshalb mit Sorge, wenn das Land für die Landesverwaltung zum Beispiel durch Bündelung von Ressourcen und Netzwerken isolierte Strukturen schafft. Demgegenüber sollte eine gemeinsame IT-Sicherheitsstrategie verfolgt werden, die die personalwirtschaftliche und infrastrukturelle Zusammenarbeit über die staatlichen Ebenen hinweg bündelt und damit den strukturellen Herausforderungen des Landes Rechnung trägt.

Die Landesregierung hat im November 2020 eine Informations- und Datensicherheitsstrategie 2023 des Landes Mecklenburg-Vorpommern verabredet, in der die Herausforderungen und Ziele der Digitalisierung und die Herausforderungen der Datensicherheit beschrieben sind. Ausfluss dieses Strategiepapiers ist die Entwicklung einer sogenannten Informations-Sicherheitsarchitektur für das Land Mecklenburg-Vorpommern. Zu diesem Zweck hat der IT-Sicherheitsbeauftragte des Landes, Herr Steffen Tambach, damit begonnen, ein IT-Sicherheitsgesetz zu entwerfen, das perspektivisch dem Landtag zur Beschlussfassung zugeleitet werden soll. Der Landkreistag als Vertreter der landkreislichen Verwaltung ist hieran beteiligt.

Aus Sicht des Landkreistages wird mit dem Handlungsansatz, eine gemeinsame Rechtsgrundlage für die Herstellung eines optimalen IT-Sicherheitsnetzes für das gesamte Land Mecklenburg-Vorpommern zu schaffen, in bundesweit innovativer und zeitgemäßer Weise auf das Thema IT-Sicherheit reagiert. Der Landkreistag betont ausdrücklich, dass die Einbeziehung des sogenannten sekundären Geltungsbereichs (der Gebietskörperschaften) bereits in der Phase der Konzeptionierung des IT-Sicherheitsgesetzes eine sehr gute Grundlage dafür schafft, dass eine gemeinsame IT-Sicherheitsstruktur für alle Ebenen der staatlichen Verwaltung entsteht.

Durch den Erlass eines IT-Sicherheitsgesetzes wird zukünftig institutionell und organisatorisch sichergestellt sein, dass ISO-Standards oder sogar die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des BSI IT-Grundschutzkompendiums in der jeweils aktuellen Fassung umgesetzt wird, dass IT-Sicherheitsstandards auf allen Verwaltungsebenen beachtet und durch entsprechende personelle Strukturen (Beauftragte, Dienstleister, Prüfinstanzen und Gremien) verantwortungsgerecht wahrgenommen werden.

Mit den im Antrag der FDP-Fraktion beschriebenen Handlungsfeldern befasst sich auch die Diskussion zu einem IT-Sicherheitsgesetz und dieses wird hierzu Antworten geben müssen.

Mit freundlichen Grüßen

M. Köpp

Matthias Köpp
Geschäftsführendes Vorstandsmitglied

ZV eGo-MV • Eckdrift 103 • 19061 Schwerin

Landtag Mecklenburg-Vorpommern
Ausschuss für Inneres, Bau und Digitalisierung
Der Vorsitzende
Lennéstraße 1
19053 Schwerin

Die Verbandsvorsteherin

Bearbeiter: Nicole Kuprat
Bereich: Verbandsvorsteherin
Telefon: 0385 / 77 33 47-10
Email: nicole.kuprat@ego-mv.de
Aktenzeichen:

Schwerin, 24. März 2022

Stellungnahme zur Drucksache 8/249 – Cyberkriminalität verhindern

Sehr geehrter Herr Vorsitzender,

wir bedanken uns für Ihr Schreiben vom 7. März 2022 und die damit verbundene Möglichkeit, zum Antrag der Fraktion der FDP: „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen“ Stellung nehmen zu dürfen.

Anliegend erhalten Sie die erbetene Stellungnahme des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern.

Unter Bezugnahme auf die Forderung der Fraktion, die Cybercrime-Dienststellen des Landes zukunftsfähig aufzustellen, möchten wir zunächst klarstellen, dass dies nur unter Einbeziehung der Kommunen gelingen kann. Bereits mehrere Vorfälle im vergangenen und aktuellen Jahr zeigen, dass die Verwaltung und die öffentliche Infrastruktur beliebte Ziele für Cyberangriffe sind. Insofern gilt es nicht nur, die Sensibilität der Bürgerinnen und Bürger sowie der Unternehmen zu erhöhen, sondern auch die Kommunen stärker zu unterstützen – sowohl dabei, geeignetes Personal für den Bereich IT-Sicherheit und Infrastruktur zu gewinnen und zu binden, als auch mit einer dauerhaft tragfähigen Finanzierungsregelung zur Gewährleistung der Informationssicherheit.

Ein wesentlicher Baustein zur Gewährleistung der Informationssicherheit im öffentlichen Sektor ist aus Sicht des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern auch eine harmonisierte und zentralisierte IT-Landschaft bzw. eine Auslagerung der kommunalen IT in ein Rechenzentrum, verbunden mit der Erhöhung des Sicherheitsniveaus. Das Land M-V sollte Bestrebungen dieser Art auch für die kommunale Familie unterstützen. Ein bereits vor Jahren angeregter IT-Konsolidierungsfonds, gerade für die finanzschwachen Kommunen, sollte demnach unabhängig von der personellen Verstärkung in Bezug auf den Bereich IT-Sicherheit und Infrastruktur realisiert werden.

Erlauben Sie uns an dieser Stelle auch einen Verweis auf die Forderungen an die Landesregierung, einer von der Verbandsversammlung des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern und dem Vorstand des Städte- und Gemeindetages Mecklenburg-Vorpommern im Rahmen der Bildung der neuen Landesregierung beschlossenen Ziel- und Maßnahmendarstellung.

Für Rückfragen stehe ich Ihnen gern zu Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Nicole Kuprat
Verbandsvorsteherin

Anlage:
Stellungnahme des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern zum Antrag der FDP-Fraktion: „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen“

Stellungnahme des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern zum Antrag der FDP-Fraktion: „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen“

Vorbemerkungen

Die Bedrohungen für die IT-gestützten Geschäftsprozesse öffentlicher Einrichtungen, kritischer Infrastrukturen und Unternehmen, aber auch für Privatpersonen, nehmen in Mecklenburg-Vorpommern stark zu. Gegenüber lokalen Medien bekräftigte zuletzt der Minister für Inneres, Bau und Digitalisierung, Herr Pegel, dass gerade vor dem Hintergrund der derzeitigen geopolitischen Herausforderungen die Aktivitäten durch kriminelle Hacker zunehmen. Daher plädierte er beispielsweise im Januar 2022 im Landtag dafür, ein Landesamt für Digitale Sicherheit aufzubauen. Dieses neu zu schaffende Landesamt solle einheitliche Standards festlegen und die IT-Sicherheit aller Landesbehörden an zentraler Stelle bündeln.
Der Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV) begrüßt dieses Vorhaben, fordert jedoch ausdrücklich, den **landesseitigen Aufbau der Informationssicherheit mit einer stärkeren Unterstützung der kommunalen Ebene zu verbinden**, so wie es auch in der Koalitionsvereinbarung zwischen SPD und DIE LINKE. Mecklenburg-Vorpommern für die 8. Legislaturperiode 2021-2026 festgehalten ist.

Mit dem steigenden Grad der technischen Vernetzung der verschiedenen Systeme und ebenenübergreifenden Kommunikation steigen auch die Verwundbarkeit und die Bedrohung durch Cyberangriffe. Insofern werden die Forderungen der Fraktion der FDP unterstützt, die verschiedensten Interessengruppen besser vor Angriffen aus dem Internet zu schützen. Als Interessenvertreter der Kommunalbehörden in Mecklenburg-Vorpommern setzt sich der eGo-MV dafür ein, dass die Kommunen im Land bei diesen Überlegungen angemessen berücksichtigt werden – diese sind sowohl in personeller als auch in finanzieller Sicht das schwächste Glied in der Kette der Informationssicherheit und damit auch mögliche und wahrscheinliche Einstiegspunkte für Angriffe, zum Beispiel auf das Verwaltungsnetz des Landes (CN LAVINE). Wir plädieren daher dafür, dass die **Maßnahmen zur Erhöhung der Cybersicherheit ebenenübergreifend aufgestellt** werden und dass den Kommunen ein beratender und beaufsichtigender **Beauftragter der Kommunalverwaltungen für Informationssicherheit (BeKVIS)** zur Seite gestellt wird – analog dem Beauftragten der Landesverwaltung für Informationssicherheit (BeLVIS). Der BeKVIS wurde erstmals in einer gemeinsamen Stellungnahme des eGo-MV und der DVZ Datenverarbeitungszentrum M-V GmbH auf den Antrag „Bürgernahe Verwaltung – papierlose Kommunikation erfordert sichere Infrastrukturen“ der Fraktionen der SPD und CDU (Drucksache 6/2928 vom 30.04.2014) sowie mehrfach in der Folgezeit dem Land gegenüber eingefordert. Eine Realisierung scheiterte bisher an ungelösten Fragen der Zuständigkeit und Refinanzierung.

Vor dem Hintergrund der gesetzlichen Verpflichtungen zur Verwaltungsdigitalisierung, zum Beispiel aufgrund des Onlinezugangsgesetzes und des E-Government-Gesetzes M-V einerseits sowie den stark steigenden Bedrohungen für die Informationssicherheit anderseits, sieht der eGo-MV das Land M-V in der Pflicht, mehr Verantwortung bei der Gewährleistung der Informationssicherheit für die Kommunen und Unternehmen zu übernehmen. Bei ebenenübergreifenden Verfahren hat diese eine besondere Bedeutung, da man einen einheitlichen Sicherheitsstand auf allen Ebenen herstellen muss. Wenn die Kommunen möglicherweise durch die EU-NIS2-Richtlinie perspektivisch zur kritischen Infrastruktur (KRITIS) zählen, werden sich die Anforderungen an die Gewährleistung der Informationssicherheit sogar nochmals erhöhen. Daher ist eine **intensivere Einbeziehung der Kommunen in die IT-Sicherheitsstrategie des Landes M-V** unbedingt erforderlich. Ergänzend sind gesetzliche Vorgaben zu schaffen, nach denen die Themen der Informationssicherheit von Behörden und Unternehmen nicht nur „mitgedacht“ werden müssen; stattdessen sollten diese Einrichtungen in gewisser Weise verpflichtet werden, die notwendigen personellen, fachlichen, zeitlichen und finanziellen Ressourcen zur Bewältigung der Aufgaben im Bereich der IT-Sicherheit vorzuhalten und den Aufsichtsbehörden entsprechend nachzuweisen. So könnte das Land M-V durch regelmäßige Auditierungen in den Kommunen den Druck zur Umsetzung der Anforderungen an die Informationssicherheit erhöhen,

Geschäftsstelle:
Eckdrift 103
19061 Schwerin

Amtsgericht Schwerin
HRA 3949

Kontakt:
Telefon 0385 / 77 33 47-0
Fax 0385 / 77 33 47-28
E-Mail info@ego-mv.de
De-Mail: poststelle@ego-mv.de-mail.de
Web www.ego-mv.de

Bankverbindung:
IBAN DE27 1203 0000 1001 1855 35
BIC BYLADEM1001
Deutsche Kreditbank Berlin
Steuer-Nr. 090/144/00882
USt.-IdNr. DE279621892

gleichzeitig aber den überprüften Kommunen bei der Beseitigung erkannter Defizite gezielt unter die Arme greifen, auch in finanzieller Hinsicht, z.B. durch (Förder-) Programme des Landes M-V oder des Bundes.

Aus unserer Erfahrung heraus ist eine ganzheitliche Informationssicherheit zum Scheitern verurteilt, wenn die Kommunen bei der Bewältigung der Herausforderungen allein gelassen werden. Die **Gewährleistung der Informationssicherheit ist keine Kernaufgabe der (kommunalen) Verwaltung**, insofern mangelt es insbesondere in kleineren Kommunen oft an fachkundigem Personal; häufig werden Verwaltungsbeschäftigte mit Themen des IT-Betriebs und der IT-Sicherheit beauftragt, die dafür nicht die erforderlichen Kompetenzen aufweisen oder zu wenig Zeitanteile für die Aufgaben der Informationssicherheit zugewiesen bekommen. Darüber hinaus gestaltet sich die Gewinnung von geeigneten Fachkräften am Arbeitsmarkt sehr schwierig: Insofern begrüßen wir ausdrücklich die Forderung der FDP-Fraktion, die Weiterentwicklung der IT-Studiengänge voranzutreiben. Zu beachten ist in diesem Zusammenhang jedoch auch, dass gut ausgebildete Fachkräfte und Hochschulabsolventen aufgrund des Gehaltsgefälles bevorzugt in die Wirtschaft oder in andere Bundesländer abwandern; Personalbindungsprogramme monetärer und nicht-monetärer Art sind daher auch und besonders für das Flächenland Mecklenburg-Vorpommern obligatorisch, um die wenigen Fachkräfte für eine Tätigkeit im öffentlichen Dienst gewinnen und halten zu können.

Ungeachtet dessen, dass die Cybercrime-Aktivitäten ebenenübergreifend ausgebaut und dafür die entsprechenden Kapazitäten vorgehalten werden müssen, kann auch die Konsolidierung der kommunalen IT zur Erhöhung des Sicherheitsniveaus beitragen. Angeregt wird in diesem Zusammengang daher, die **Standardisierung und Zentralisierung der kommunalen Informationstechnik in kompetenten Händen** durch das Land M-V voranzutreiben. Von Sonderlösungen wird den Kommunen auch heute schon grundsätzlich abgeraten; die notwendige Konsolidierung der kommunalen IT ist bereits von vielen erkannt worden. Die Kooperation über Amts-, Stadt- und Kreisgrenzen hinweg, beispielsweise im Rahmen der interkommunalen Zusammenarbeit, muss weiter verstärkt werden, damit der Verantwortungsdruck der kommunalen Administratoren reduziert und ihnen gleichzeitig mehr Ressourcen für den lokalen IT- und Anwendersupport ermöglicht werden. In diesem Zusammenhang ist aber zwingend die Frage der Finanzierung und einer bereits geforderten Unterstützung durch das Land zu klären.

Alle vorweg genannten Maßnahmen würden aus unserer Sicht die Basis dafür schaffen, die digitale Souveränität in den Behörden und Unternehmen zu stärken – was übrigens bezogen auf die Behörden eine der zentralen Forderungen des IT-Planungsrates ist. Die Umsetzung dieser Maßnahmen erhöht die digitalen Kompetenzen auf kommunaler Ebene und in den Unternehmen; damit entstünde ein Mehrwert an den gemeinsamen Schnittstellen der öffentlichen Hand und der Wirtschaft bzw. der Bürgerinnen und Bürger.

Wir möchten nun wie gewünscht zu den konkreten Forderungen der Fraktion der FDP Stellung beziehen:

1. **Bereitstellung von mehr gut ausgebildetem Personal für den Bereich IT-Sicherheit und Infrastruktur**

Mehr Personal mit der erforderlichen Ausbildung wird vom eGo-MV aufgrund der eingangs beschriebenen Herausforderungen ausdrücklich begrüßt. Die Ausbildung der Fachkräfte muss dabei in der für die aktuellen und künftigen Aufgaben erforderlichen Breite erfolgen, wobei das Land M-V in der Verantwortung ist, die dafür erforderlichen Ausbildungs- und Studiengänge zu organisieren, bereitzustellen und entsprechend zu finanzieren. Die Ausbildungsinhalte müssen auf die aktuellen und künftigen Anforderungen in der IT-Branche ausgerichtet und ständig weiterentwickelt werden. Die Kapazitäten der Hochschulen und Ausbildungsbetriebe müssen so gestaltet werden, dass mit den Absolventen perspektivisch Fachkräfte in angemessener Anzahl zur Verfügung stehen.

Bei den Schulabsolventen sollte das Land M-V intensiv für IT-nahe Ausbildungen und Studiengänge werben – verbunden mit der Aussicht auf krisensichere Arbeitsplätze in Behörden auf kommunaler oder Landesebene. Arbeitgeber des öffentlichen Dienstes sollten sich zunehmend bei Berufs- und Berufsbildungsmessen engagieren; der eGo-MV würde bei landesweit koordinierten Aktionen seine Bereitschaft erklären, sich zu beteiligen. Denkbar in diesem Zusammenhang ist auch, verstärkt Seiteneinsteiger aus anderen Branchen anzuwerben, um die Lücken beim Fachpersonal zu schließen.

Der Bund sollte darüber hinaus aber auch mehr Mittel und Werbung für Weiterbildungsprogramme in Kommunen und Unternehmen bereitstellen. Vorhandene Weiterbildungsangebote, z.B. von der Bundesakademie für öffentliche Verwaltung (BAköV), sollten ausgebaut und die Weiterbildungskosten ganz oder teilweise, beispielsweise durch den IT-Planungsrat, getragen werden.

Wie in den Vorbemerkungen erwähnt, muss der öffentliche Dienst des Landes und der Kommunen aber auch bei der Entgeltgestaltung für hochkarätige Arbeitskräfte flexibilisiert werden; innerhalb der starren Grenzen der Tarifverträge ist der öffentliche Dienst im Wettbewerb um die besten Köpfe nicht konkurrenzfähig zur Privatwirtschaft.

2. Weiterentwicklung der IT-Studiengänge gemeinsam mit den Hochschulen des Landes

Zunächst empfehlen wir zur Schließung der Lücken im Fachpersonal, die IT-nahen Studienplätze im Land zu erhöhen. Die Studieninhalte müssen sodann ständig an die aktuellen und künftigen Herausforderungen der IT-Branche angepasst und erweitert werden. Wichtig in diesem Zusammenhang ist jedoch auch, dass das Lehr- und ggf. Verwaltungspersonal der Hochschulen im angemessenen Umfang bereitstehen muss, um die Erhöhung der Studienplätze bewältigen zu können. Die Organisation sowie die Finanzierung dessen sehen wir beim Land.

Der eGo-MV ist zur Zusammenarbeit bei der (Weiter-)Entwicklung der IT-Studiengänge bereit und würde den Hochschulen eine fachliche und organisatorische Mitwirkung im Rahmen seiner Kompetenzen anbieten, beispielsweise auf dem Gebiet des Datenschutzes und der IT-Sicherheit. Gern bringen wir unsere fachlichen und praktischen Erfahrungen ein, um damit zur Gestaltung der Lehrinhalte beitragen zu können. Weiter bietet der Zweckverband seine aktive Mitarbeit zur Weiterentwicklung der IT- und Verwaltungsstudiengänge an, beispielsweise durch inhaltliche Beiträge zur Fortschreibung der Ausbildungskonzepte und Lehrpläne, regelmäßige Gastvorlesungen, studienbegleitende Praktika oder Betreuung von Abschlussarbeiten. Damit könnte gleichzeitig die Möglichkeit geschaffen werden, Fachkräfte für Kommunalbehörden zu gewinnen (vgl. oben skizzierte Ausführungen zur 1. Forderung der FDP-Fraktion).

3. Angriffe besser vereiteln, Täter identifizieren, verfolgen und zur Rechenschaft ziehen

Der Verfassungsschutzverbund, der Verwaltungs-Verbund des Computer Emergency Response Teams (Verwaltungs-CERT-Verbund) sowie das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind bereits sehr aktiv bei der forensischen Analyse von Angriffen, um den Selbstschutz von Behörden auf Bundes-, Landes- und Kommunalebene zu verbessern. Die unverzügliche Übernahme dieser wertvollen Vorarbeiten ist in der Praxis allerdings mit Problemen behaftet, vgl. Ausführungen zu den fachlichen, personellen und zeitlichen Limitierungen unter Vorbemerkungen.

Die IT-Sicherheitsstrategie des Landes muss transparent organisiert und permanent weiterentwickelt werden; wobei Kommunen und KRITIS stärker in die Landesstrategie einbezogen und unterstützt werden müssen. Immer wieder stellen wir fest, dass die Informationsflüsse derzeit noch sehr unkoordiniert sind; sicherheitsrelevante Informationen sind daher in praxistauglichen Prozessen auf vertraulichem Wege effizient zu verteilen. Das trifft insbesondere zu, wenn Cyberangriffe bzw. Sicherheitslücken in IT-Systemen frühzeitig erkannt werden. Neben der Erforderlichkeit, die Kommunen in geeigneter Weise in den CERT-Informationsverbund einzubinden, muss sichergestellt werden, dass Informationen ebenenübergreifend und zielgerichtet weitergegeben werden – auch hier wäre der zuvor genannte BeKVIS von Vorteil.

Gesetzliche Vorgaben, wie zum Beispiel das in Arbeit befindliche IT-Sicherheitsgesetz M-V, müssen dabei auch für kleinere Kommunen im Hinblick auf das verfügbare Personal und die Finanzierung der erforderlichen Sicherheitsmaßnahmen realisierbar sein. Die Kommunen müssen in die Lage versetzt werden, den steigenden Anforderungen der Digitalisierung und damit verbunden der Gewährleistung der IT-Sicherheit gerecht zu werden, ohne dass dies die kommunalen Haushalte übermäßig belastet.

IT-Angriffe zu vereiteln, bereitet in der kommunalen Praxis häufig Schwierigkeiten: Das IT-Personal ist im Regelfall mit dem aktiven Selbstschutz überfordert – sei es, weil eine kompetente und zielgenaue Konfiguration der Firewall, das Erkennen und Verhindern von Angriffen oder die rasche Wiederherstellung der Arbeitsfähigkeit nach Sicherheitsvorfällen handwerklich nicht bekannt sind, nicht mit funktionierenden Prozessen hinterlegt und häufig auch nicht geübt werden. Um dem entgegenzuwirken, hat der eGo-MV schon frühzeitig ein breites Sensibilisierungs- und Unterstützungsangebot für die Kommunen aufgebaut. Sofern die vom Zweckverband empfohlenen organisatorischen und technischen Präventionsmaßnahmen von den Kommunen umgesetzt werden, können bereits viele Angriffe vereitelt oder zumindest deren Auswirkungen erheblich reduziert werden. Wir arbeiten ständig daran, die Maßnahmen im Kontext aktueller Herausforderungen auszubauen. Dazu sind wir allerdings sehr stark darauf angewiesen, die erforderlichen Informationen von übergeordneten Stellen zeitnah zu erhalten.

Zugleich hat der eGo-MV in der Vergangenheit ständig darauf hingewirkt, die Vernetzung der kommunalen IT-Administratoren untereinander zu verbessern. Dazu werden u.a. regelmäßige Erfahrungsaustausche organisiert und Themen technischer, rechtlicher und z.T. auch politischer Art vermittelt, die die Administratoren bei der Bewältigung ihrer täglichen Herausforderungen vor Ort unterstützt. Darüber hinaus halten wir es für angebracht, dass auch das Land M-V in seiner Verantwortung für die kommunale Ebene eine breite Aufklärungs- und Schulungsarbeit bei den lokalen IT-Administratoren organisiert; bei der Planung und Umsetzung unterstützen wir gern.

Bei der Verfolgung der Täter kann der eGo-MV nur bedingt Unterstützung leisten. Die IT-Angriffe erfolgen in der Regel aus anderen Ländern heraus; die Strafverfolgung obliegt dem Bundeskriminalamt, ggf. dem Landeskriminalamt M-V und beispielsweise auch Europol. Damit die genannten Behörden internationale Straftaten im Zusammenhang mit IT-Angriffen angemessen bewältigen können, benötigen natürlich auch diese ausreichend fachkompetentes Personal.
Der eGo-MV kann jedoch auch aus eigener Erfahrung berichten, dass durch Internetkriminalität geschädigte Einrichtungen oft regelrecht dazu gedrängt werden müssen, eine Strafanzeige aufgrund von Computersabotage nach § 303b Strafgesetzbuch zu erstatten. Ohne eine solche Anzeige wird die Wahrscheinlichkeit erheblich reduziert, dass die Straftaten aufgeklärt werden können. Hier sehen wir die Strafverfolgungsbehörden, aber auch die (kommunalen) IT-Dienstleister in der Pflicht, ihre Kunden entsprechend für die Notwendigkeit der Erstattung von Anzeigen bei entdeckten Cybercrime-Aktivitäten zu sensibilisieren. Aus unserer Sicht muss daher z.B. auch das Landeskriminalamt M-V verstärkt gegenüber Kommunen, Unternehmen sowie Bürgerinnen und Bürgern über den Straftatbestand der Computersabotage aufklären. Vielen der Adressaten ist gar nicht bewusst, dass IT-Angriffe zur Anzeige gebracht werden sollten; in diesem Sinne ist mehr Öffentlichkeitsarbeit seitens des Landeskriminalamtes M-V wünschenswert. Im Rahmen der IT-Sicherheitsstrategie des Landes M-V sollte ggf. auch das Ministerium für Inneres, Bau und Digitalisierung gewährleisten, dass die für die Adressaten erforderlichen Informationen zur Strafverfolgung bereitgestellt werden, um dort dem Sicherheits- und Kompetenzbedürfnis Rechnung zu tragen.

4. Cybercrime-Dienststellen in den Behörden des Landes besser ausstatten und landesweit koordinieren

In diesem Zusammenhang betonen wir nochmals die Erforderlichkeit, dass die Maßnahmen zur Erhöhung der Cybersicherheit ebenenübergreifend aufgestellt und dafür alle beteiligten Stellen über ausreichend Personal mit den erforderlichen fachlichen Kompetenzen ausgestattet werden müssen. In die landesweite Koordination durch die Cybercrime-Dienststellen müssen die Kommunen, der eGo-MV sowie die kommunalen Spitzenverbände zwingend einbezogen werden. Zwar arbeiten wir auf

Arbeitsebene bereits seit mehreren Jahren sehr intensiv und produktiv mit dem Computer Emergency Response Team des Landes (CERT M-V) zusammen, es ist aber deutlich erkennbar, dass das CERT M-V nach wie vor primär auf die Landesressorts ausgerichtet ist und dort priorisiert mit seiner Fachkompetenz unterstützt. Aus unserer Sicht muss das CERT M-V mit einem erweiterten Fokus neu ausgerichtet werden, so dass neben den Landesbehörden auch die Kommunen und Unternehmen im Land angemessen Berücksichtigung finden.
Zu besseren Koordinierung der Abwehr von Cybercrime-Aktivitäten im behördlichen Umfeld verweisen wir dabei erneut auf die unter den Vorbemerkungen gemachten Ausführungen zur Einführung des „Beauftragten der Kommunalverwaltung für Informationssicherheit (BeKVIS)“. Diese als Einzelperson oder als Lenkungsgremium organisierte Funktion sollte intensiv mit dem Landes-Äquivalent, dem BeLVIS, zusammenarbeiten, um gemeinsam die Bedrohungen für die ministerialen und kommunalen Behörden erkennen, einschätzen und durch koordinierte Maßnahmen begegnen zu können.

Das CERT M-V arbeitet länderübergreifend mit anderen CERTs, dem Bundeskriminalamt sowie den Landeskriminalämtern zusammen. Aus unserer Sicht ist es aber erforderlich, dass bei dieser länderübergreifenden Zusammenarbeit insbesondere auch die Kommunen einbezogen und vernetzt werden. Es ist überdies vorstellbar, dass perspektivisch auch eine Vernetzung mit dem Cyber- und Informationsraum der Bundeswehr (CIR Bundeswehr) aufgebaut wird, um auch auf dieser Ebene relevante Informationen zum Selbstschutz von Landes- und Kommunalbehörden sowie Gewerbetreibenden auszutauschen. Auch dies müsste im Rahmen der landesweiten Koordinierung der ebenenübergreifenden Informationssicherheit geregelt und organisiert werden.

5. Sensibilität der Bürgerinnen und Bürger, Kommunen, Unternehmen und ihrer Beschäftigten erhöhen; Beratungsangebote für Bürgerinnen und Bürger sowie Unternehmen ermöglichen

Die Sensibilisierung und Beratung der genannten Benutzergruppen ist eine wesentliche Voraussetzung, um den aktuellen Gefährdungen im Hinblick auf die Informationssicherheit angemessen begegnen zu können, sich entsprechend vorzubereiten und im Ernstfall reagieren zu können. Als aktuelles Beispiel sei an dieser Stelle auf die erhöhte IT-Bedrohungslage durch die geopolitischen Spannungen in Osteuropa verwiesen.

Wie bereits vorweg angemahnt, dürfen auch hier die kommunalen Körperschaften nicht vergessen werden; diese müssen in Beratungs- und Sensibilisierungsmaßnahmen des Landes M-V unbedingt einbezogen werden. Ziel solcher Angebote muss sein, die Kompetenzen im Bereich der digitalen Souveränität und der Informationssicherheit zu erhöhen.
Die Arbeitsfähigkeit der Kommunen wird durch die steigenden IT-Bedrohungen immer häufiger eingeschränkt, wie bekannte Fälle aus dem vergangenen und aktuellen Jahr zeigen. Dabei ist diese der Garant dafür, dass beispielweise auch Gewerbetreibende ihre Geschäfte ordnungsgemäß durchführen können – z.B. im Hinblick auf die Nutzung von Services der Verwaltung, wie Gewerbeanmeldung, gewerbliche Kfz-Zulassung, Baugenehmigungen usw.

Für Bürgerinnen und Bürger bzw. Unternehmen gibt es bereits vielfältige Sensibilisierungsangebote, die von den verschiedenen Zielgruppen auch unterschiedlich stark in Anspruch genommen werden, beispielweise:

- „BSI für Bürger“: gutes und laienverständliches Informationsangebot des BSI – u.a. mit dem Newsletter „sicher informiert“, Tipps, Empfehlungen; ergänzende, publikumswirksame Aktivitäten des BSI u.a. bei Twitter und Facebook
- polizeiliche Kriminalitätsprävention der Länder und des Bundes; https://www.polizei-beratung.de/
- Projekt „Medienscouts MV“ des Landesbeauftragten für Datenschutz und Informationsfreiheit in M-V zur Sensibilisierung von Kindern und Jugendlichen; https://www.medienscouts-mv.de/
- Medienanstalt M-V mit diversen Projekten zur Förderung der Medienkompetenz bei Kindern und Jugendlichen; https://medienanstalt-mv.de/medienkompetenz/medienkompetenz.html

- Allianz für Cybersicherheit (eine Initiative des BSI), u.a. mit Informationsangeboten gezielt für die Wirtschaft
- Initiative „Deutschland sicher im Netz“ des Bundesministeriums des Innern und für Heimat mit vielfältigen Informationen für Verbraucherinnen, Verbraucher und Gewerbetreibende.

Als bereits vorhandene Beratungsangebote für die kommunale Ebene möchten wir hervorheben:

- jährliche Durchführung einer „Hacker-Roadshow“ des Ministeriums für Inneres, Bau und Digitalisierung M-V in Zusammenarbeit mit dem eGo-MV zur Sensibilisierung von Bediensteten der Landes- und Kommunalverwaltungen in M-V aus Mitteln des IT-Planungsrates
- Tagungsreihe „Medienaktiv“ des Landesbeauftragten für Datenschutz und Informationsfreiheit in M-V für wechselnde Zielgruppen, z.B. Kinder und Jugendliche, Seniorinnen und Senioren, Beschäftigte usw.

Die Kommunen erhalten darüber hinaus bereits tatkräftige Unterstützung durch das CERT M-V und den eGo-MV; so informiert beispielsweise das CERT M-V Landes- und Kommunalbehörden zu aktuellen Gefährdungen der Informationssicherheit und stellt anlassbezogene Hilfestellungen bereit. Auch der eGo-MV bietet Schulungen primär für Kommunen, nachgeordnete kommunale Einrichtungen und staatliche Schulen, grundsätzlich aber auch für Dritte auf dem Gebiet des Datenschutzes und der Informationssicherheit an, allerdings werden die Angebote aufgrund von personellen, zeitlichen und finanziellen Restriktionen seitens der Kommunen oft nicht im erforderlichen Umfang wahrgenommen. Damit sich die Kommunen angemessen auf aktuelle und künftige Bedrohungen einstellen können, benötigen sie eine angemessene Personalausstattung. Die Adressaten dürfen dabei jedoch nicht auf den diesbezüglichen Kosten sitzen bleiben, vielmehr muss das Land M-V angemessen unterstützen, wie schon mehrfach ausgeführt.

Die IT-Sicherheitsstrategie des Landes M-V sollte darüber hinaus Maßnahmen für eine gezielte Ansprache der Adressaten beinhalten. Dabei sollten aus unserer Sicht auch die relevanten Verbände, Vereine sowie die Industrie- und Handelskammern einbezogen werden, wie es auch die FDP-Fraktion fordert.

Fazit:

Die Informationssicherheit gewinnt zunehmend an Bedeutung. Mit Blick auf die dynamischen Herausforderungen in Bezug auf die Angriffe aus dem Internet sollten alle Ebenen des Landes sowie Bürgerinnen und Bürger und Unternehmen für den Ernstfall gewappnet sein. Daher ist es einerseits unbedingt erforderlich, die Sensibilisierung der Bevölkerung und der Wirtschaft für das Thema voranzutreiben. Andererseits bedarf es einer abgestimmten ebenenübergreifenden Vorgehensweise; Land und Kommunen müssen an einem Strang ziehen und gemeinsame Strategien und Standards entwickeln, bei deren Umsetzung auch die Kommunen sowohl in personeller als auch finanzieller Hinsicht tatkräftig unterstützt werden müssen. Gleichzeitig sind Konzepte zu erarbeiten, um mehr fachkundiges Personal für das Thema zu gewinnen.

Die Empfehlungen des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern zur Umsetzung der Forderungen der Fraktion der FDP lauten zusammengefasst:

- Die Informationssicherheit ist vor dem Hintergrund steigender Anforderungen auf allen Ebenen zu gewährleisten. Die Kommunen müssen unterstützt werden, den steigenden Herausforderungen gerecht zu werden, ohne dass dies die Haushalte übermäßig belastet.
- Um präventive Maßnahmen ergreifen und somit Angriffe besser vereiteln zu können, müssen alle beteiligten Stellen mit ausreichend fachlicher Kompetenz und finanziellen Kapazitäten ausgestattet sein.
- Die Personalsituation ist und bleibt für die Behörden kritisch; es wird immer schwieriger, geeignetes IT-Personal zu gewinnen. Um erfahrene Fachkräfte zu einer Anstellung bzw. einem Wechsel aus Wirtschaftsunternehmen in die öffentliche Verwaltung zu bewegen, bedarf es

neben Konzepten zur Aus- und Weiterbildung auch zukunftsfähiger Personalgewinnungs- und -bindungsmaßnahmen.

- Die IT-Sicherheitsstrategie des Landes M-V muss Aufklärungskampagnen für Bürgerinnen und Bürger, Gewerbetreibende sowie Kommunen entwickeln, auch vor dem Hintergrund, Täter identifizieren und zur Rechenschaft ziehen zu können. Daneben müssen zu diesem Zweck weitere Zielgruppen erschlossen werden: Wir halten die Einbeziehung schulischer, wissenschaftlicher und sozialer Einrichtungen (Kita, Hort, Pflege) für dringend erforderlich.
- Die IT-Sicherheitsstrategie des Landes sollte Kommunen stärker in die Kommunikation mit Bürgerinnen und Bürgern einbeziehen: Kommunen sind die primären Ansprechpartner und Anlaufstellen der Bürgerinnen und Bürgern vor Ort und damit eine ideale Kontakt- und Vermittlungsstelle. Insofern sollten bereits die kommunalen Beschäftigten sensibilisiert sein und bestenfalls Informationsmaterial zum Thema Cybersicherheit bereitgestellt werden – zum Beispiel analog zum Aufklärungsmaterial in den Einwohnermeldeämtern zum Organspenderegister.
- Cybercrime-Dienststellen aller Ebenen sind landesweit zu koordinieren. Betreiber kritischer Infrastrukturen müssen besser in die tägliche Kommunikation und Koordinierung einbezogen werden. Darunter sind auch die Kommunen zu verstehen.

Gern stehen wir Ihnen für Rückfragen oder weiterführende Erläuterungen zu den vorgenannten Ausführungen zur Verfügung.

Geschäftsstelle:
Eckdrift 103
19061 Schwerin

Amtsgericht Schwerin
HRA 3949

Kontakt:
Telefon 0385 / 77 33 47-0
Fax 0385 / 77 33 47-28
E-Mail info@ego-mv.de
De-Mail: poststelle@ego-mv.de-mail.de
Web www.ego-mv.de

Bankverbindung:
IBAN DE27 1203 0000 1001 1855 35
BIC BYLADEM1001
Deutsche Kreditbank Berlin
Steuer-Nr. 090/144/00882
USt.-IdNr. DE279621892

DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH

DVZ M-V GmbH, Lübecker Str. 283, 19059 Schwerin

Landtag Mecklenburg-Vorpommern
Ausschuss für Inneres, Bau und Digitalisierung
Der Vorsitzende – Herrn Ralf Mucha
Lennéstraße 1 (Schloss)
19053 Schwerin

IHR ZEICHEN: -
UNSER ZEICHEN: -
ANSPRECHPARTNER: *Ralf Prigandt*
TELEFON: *0385 4800 297*
TELEFAX: *0385 4800 487*
E-MAIL: *r.prigandt@dvz-mv.de*

DATUM: *24. März 2022*

Anhörung zum Antrag der Fraktion der FDP

Cyberkriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen

Stellungnahme der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH

Sehr geehrter Herr Mucha,

ich bedanke mich bei Ihnen für die Einladung zur öffentlichen Anhörung des Ausschusses für Inneres, Bau und Digitalisierung am 31. März 2022. Da ich persönlich leider verhindert bin, wird mich Herr Ralf Prigandt, Abteilungsleiter für den Bereich IT-Security in der DVZ M-V GmbH, bei der Anhörung vertreten. Die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH begrüßt den Antrag der FDP-Fraktion und nimmt nachfolgend Bezug.

1. „Die Landesregierung wird aufgefordert, mehr gut ausgebildetes Personal für den Bereich IT-Sicherheit und Infrastruktur bereit zu stellen“.

Der Arbeitsmarkt rund um IT-Personal, insbesondere im Bereich IT-Sicherheit, ist sehr begrenzt und ausreichend qualifiziertes Personal ist nur schwer zu rekrutieren.

Der Fokus sollte nicht ausschließlich auf die Schaffung und Besetzung zusätzlicher Stellen gelegt werden, sondern auch verstärkt auf die Personalentwicklung und Personalbindung. Es ist empfehlenswert vorhandene Kompetenzen zu Bündeln und Knowhow auszubauen.

Die DVZ M-V GmbH hat in 2021 eine Umstrukturierung umgesetzt um den Erfordernissen gerecht zu werden. So wurde eine extra Abteilung für alle Belange der IT-Security geschaffen.

Auch die Bündelung der IT-Kompetenzen der Landesverwaltung im vorgesehenen Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZD MV) als neuem Landesamt sehen wir dabei als richtigen Schritt zur Effizienzsteigerung und Nutzung der Personalressourcen. Dazu hat die DVZ M-V GmbH gemeinsam mit der Landesverwaltung M-V in 2021 eine Workshop-Reihe gestartet.

Die DVZ M-V GmbH hat zudem einen Außenstandort in Rostock geschaffen, um das Einzugsgebiet für Personal zu erweitern. Um die fehlende Attraktivität der Standorte in Mecklenburg-Vorpommern auszugleichen werden insbesondere auch neue Arbeitsmodelle der Zukunft Berücksichtigung finden.

2. **„Die Landesregierung wird aufgefordert, gemeinsam mit den Hochschulen des Landes ein Konzept zu entwickeln, die Weiterentwicklung der IT-Studiengänge voranzutreiben sowie entsprechende Stipendienprogramme aufzulegen."**

Eine Kooperation mit den Hochschulen sieht die DVZ M-V GmbH als große Chance. In der DVZ M-V GmbH selbst setzten wir zunehmend auf das Modell des dualen Studiums und Werkstudenten als Einstieg. Es hat sich gezeigt, dass es in diesem Modell insbesondere auf die Praxisnähe ankommt. Eine enge Kommunikation mit den Hochschulen ist daher unabdingbar.

Der Fokus sollte dennoch nicht nur auf Berufseinsteiger gelegt werden, sondern ebenso die Entwicklung von vorhandenem Personal beinhalten. Der Arbeitsmarkt wird sich durch die zunehmende Digitalisierung und den Einsatz neuer Technologien, wie z. B. künstliche Intelligenz, in seinen Anforderungen verändern. Alle Beschäftigten müssen auf diesem Weg adäquate Unterstützung finden.

3. **„Die Landesregierung wird aufgefordert, Strategien zu entwickeln um Angriffe besser zu vereiteln und die Täter zu identifizieren, zu verfolgen und zur Rechenschaft zu ziehen."**

Um Cyber-Angriffe zu vereiteln und im Ernstfall bis zur Strafverfolgung zu behandeln sind weitreichende Grundlagen zwingend erforderlich.

Im Folgenden führt die DVZ M-V GmbH aus ihrer Sicht wesentliche Grundlagen auf, welche uns durch die Landesverwaltung zur Verfügung gestellt werden muss.

Verabschiedete Rechtsverordnung zur Legitimierung des Handelns

  - Ermächtigung zur flächendeckenden und vollständigen Protokollierung und Analyse von Systemen und Netzen
  - Ertüchtigung zur Sofortreaktion bei detektierten Sicherheitsereignissen
- Verabschiedung einer Gesamtstrategie inklusive IT-Sicherheits-Strategie
- Strategie zur Kontrolle der Einhaltung von Vorgaben bzw. zur Sanktionierung bei Missachtung der Vorgaben
- Sicherstellung einer zentralen Finanzierung
- Ermächtigung zur eigenverantwortlichen Umsetzung der Gesamtstrategie

Die Handlungsfähigkeit und Legitimation aller involvierten Stellen muss kurzfristig sichergestellt werden um eine höhere Geschwindigkeit in der Detektion und der anschließenden Behandlung von Cyber-Angriffen zu erlangen.

Aus den komplexen zugrundeliegenden Anforderungen sowie der Personalsituation ergibt sich außerdem, dass alle IT-sicherheitsrelevanten Bereiche im Land eng verzahnt zusammenarbeiten müssen. Wir sind darauf angewiesen, IT-Security-Ressourcen effizient einzusetzen um den zunehmenden Cyber-Angriffen Stand zu halten.

Auch heute steht die DVZ M-V GmbH in engem Austausch mit der Landes- und Kommunalverwaltung M-V, wenn es um die Unterstützung bei IT-Sicherheitsvorfallbehandlungen geht. So werden Erkenntnisse der DVZ M-V GmbH sofort den entsprechenden Sicherheitsbeauftragen der Behörden, dem CERT M-V, bzw., auch der Polizei, zur weiteren Strafverfolgung angezeigt. Ein DVZ-eigenes Forensik-Team unterstützt die zuständigen Behörden bei der notwendigen Aufklärung.

4. „Die Landesregierung wird aufgefordert, Cybercrime-Dienststellen in den Behörden des Landes besser auszustatten und landesweit zu koordinieren."

Wie in Punkt 3 bereits erwähnt, sieht die DVZ M-V GmbH eine übergreifende Koordinierung als zwingend erforderlich an. Es muss gewährleistet werden, dass gesetzte IT-Security-Standards und –Vorgaben umgesetzt, überprüft und ggf. sanktioniert werden.

Dafür ist es auch erforderlich, geschultes Personal in den Behörden bereitzuhalten und feste Ansprechpartner zu etablieren.

Die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden durch die DVZ M-V GmbH umgesetzt und regelmäßig zertifiziert (die DVZ M-V GmbH ist nach ISO 27001 BSI-Grundschutz zertifiziert).

Neben der Ausstattung der Cybercrime-Dienststellen ist das Thema Notfallmanagement elementar. Jede Behörde muss befähigt werden, dass allen Beteiligen transparent ist,

SITZ DER GESELLSCHAFT: Schwerin
EINTRAG IM HANDELSREGISTER: HRB 187 / Amtsgericht Schwerin
GESCHÄFTSFÜHRER: Dipl.-Ing. Dipl.-Jur. Hubert Ludwig
AUFSICHTSRATSVORSITZENDE: Staatssekretärin Ina-Maria Ulbrich
UMSATZSTEUER ID-NR.: DE 13 77 33 413

NORD/LB: IBAN DE 32 2505 0000 0121 0150 69
DEUTSCHE KREDITBANK AG: IBAN DE 66 1203 0000 0010 2041 21
COMMERZBANK: IBAN DE 74 1408 0000 0250 8990 00
DEUTSCHE BANK AG: IBAN DE 85 1307 0000 0300 5279 00

POSTFACH: 120141, 19018 Schwerin ANSCHRIFT: Lübecker Straße 283, 19059 Schwerin TELEFON: +49 385 4800-0 TELEFAX: +49 385 4800-487 INTERNET: www.dvz-mv.de

was in einer Notsituation zu tun ist. Ein kompetentes Notfallteam übernimmt die Koordinierung im Angriffsfall. Dieses ist derzeit nicht vollumfänglich ausgestattet, um z. B. Rufbereitschaften 24 / 7 365 Tage abzusichern um bedarf weiterer Anstrengungen.

Die DVZ M-V GmbH konzeptioniert, erweitert und befähigt intern derzeit ein spezielles IT-Security-Notfallmanagement-Team um den gestiegenen und veränderten Cyberangriffs-Szenarien adäquat zu begegnen.

5. **„Die Landesregierung wird aufgefordert, in Zusammenarbeit mit Sicherheitsbehörden, spezialisierten Verbänden und Vereinen sowie den Industrie- und Handelskammern die Sensibilität der Bürgerinnen und Bürger, Kommunen, Unternehmen und ihrer Beschäftigten weiter zu erhöhen sowie Beratungsangebote für Bürgerinnen und Bürger als auch Unternehmen zu ermöglichen oder zu unterstützen."**

Beratungsangebote zur Sensibilisierung der unterschiedlichen Zielgruppen sind aus Sicht der DVZ M-V GmbH grundlegende Elemente, um ein hinreichendes Sicherheitsbewusstsein insbesondere bei den Behördenleitungen bzw. Geschäftsführern zu schaffen, indem Gefährdungen transparent gemacht und erforderliche Sicherheitsmaßnahmen, inklusive passender Verhaltensweisen publiziert werden. Die Gesamtverantwortung verbleibt letztendlich bei der Leitung der Institutionen.

In diesem Kontext sehen wir für die Behörden der Landes- und Kommunalverwaltungen in M-V eine zentrale Rolle beim CERT M-V (Computer Emergency Response Team), dem in seiner Dienste-Spezifikation unter anderem die Themenbereiche Warn- und Informationsdienst, Wissensmanagement, Technologieüberwachung, Sensibilisierung des Sicherheitsbewusstseins sowie Ausbildung / Schulung als Basisleistungen aufgegeben sind.

Die DVZ M-V GmbH selbst führt dafür mit ihren Mitarbeitenden regelmäßig interaktive Awareness-Kampagnen durch und bietet solche auch für die Landesverwaltung M-V an.

Alle technischen und organisatorischen Maßnahmen zur Vermeidung von Sicherheitsereignissen werden nur ganzheitlich wirksam, wenn sie korrekt durch die Beschäftigten umgesetzt und angewendet werden.

Schlusswort

Im IT-Sicherheitslagebericht des BSI wird folgendes passendes Fazit gezogen:

SITZ DER GESELLSCHAFT: Schwerin
EINTRAG IM HANDELSREGISTER: HRB 187 / Amtsgericht Schwerin
GESCHÄFTSFÜHRER: Dipl.-Ing. Dipl.-Jur. Hubert Ludwig
AUFSICHTSRATSVORSITZENDE: Staatssekretärin Ina-Maria Ulbrich
UMSATZSTEUER ID-NR.: DE 13 77 33 413

NORD/LB: IBAN DE 32 2505 0000 0121 0150 69
DEUTSCHE KREDITBANK AG: IBAN DE 66 1203 0000 0010 2041 21
COMMERZBANK: IBAN DE 74 1408 0000 0250 8990 00
DEUTSCHE BANK AG: IBAN DE 85 1307 0000 0300 5279 00

POSTFACH: 120141, 19018 Schwerin ANSCHRIFT: Lübecker Straße 283, 19059 Schwerin TELEFON: +49 385 4800-0 TELEFAX: +49 385 4800-487 INTERNET: www.dvz-mv.de

DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH

„Auch vor dem Hintergrund der angespannten Gefährdungslage kann die Digitalisierung sicher gestaltet werden. Das Eindringen von Digitalisierung in alle Lebens- und Wirtschaftsbereiche bedeutet, dass sich Cyber-Sicherheit weiterentwickeln muss. Für einen starken und auch in Zukunft sicheren Standort Deutschland ist es notwendig, die Chancen der Digitalisierung aufzugreifen und zugleich den potenziellen Risiken von Beginn an angemessen zu begegnen."

Das Fazit des Bundesamts für Sicherheit in der Informationstechnik verdeutlicht die aktuelle Lage und bestätigt nochmal die o. g. Ansätze. Informationssicherheit ist ein kontinuierlicher Prozess und bedarf darum permanenter Anpassung. Wir müssen zusammenarbeiten und Grundlagen schaffen, um den Entwicklungen in der Digitalisierung und den damit verbundenen Chancen und Risiken vorbereitet zu begegnen.

Mit freundlichen Grüßen

DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH
Geschäftsführer

H. Ludwig

SITZ DER GESELLSCHAFT: Schwerin
EINTRAG IM HANDELSREGISTER: HRB 187 / Amtsgericht Schwerin
GESCHÄFTSFÜHRER: Dipl.-Ing. Dipl.-Jur. Hubert Ludwig
AUFSICHTSRATSVORSITZENDE: Staatssekretärin Ina-Maria Ulbrich
UMSATZSTEUER ID-NR.: DE 13 77 33 413

NORD/LB: IBAN DE 32 2505 0000 0121 0150 69
DEUTSCHE KREDITBANK AG: IBAN DE 66 1203 0000 0010 2041 21
COMMERZBANK: IBAN DE 74 1408 0000 0250 8990 00
DEUTSCHE BANK AG: IBAN DE 85 1307 0000 0300 5279 00

POSTFACH: 120141, 19018 Schwerin ANSCHRIFT: Lübecker Straße 283, 19059 Schwerin TELEFON: +49 385 4800-0 TELEFAX: +49 385 4800-487 INTERNET: www.dvz-mv.de

Hanse- und Universitätsstadt Rostock

Amt für Digitalisierung und IT

Sven Bradtke

Rostock, 23.03.2022

Stellungnahme zum Antrag der Fraktion der FDP

Drucksache 8/249

Cyberkriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen

Mit zunehmender Vernetzung der unterschiedlichen IT-Komponenten in der voranschreitenden digitalen Welt wandelt sich der Anspruch an die IT-Sicherheit von primär nach innen gerichteten Sicherheitsmaßnahmen zusätzlich zu Maßnahmen, die vor äußeren Einflüssen schützen sowie Analysetechniken, die auffällige Aktivitäten in eigenen Infrastrukturen ermitteln.

EU-Projekte z.B. beschäftigen sich in diesem Umfeld mit dem Einsatz von künstlichen Intelligenzen.

„Gegen Angriffe auf die IT hilft nur eine bessere Verteidigung und mehr Resilienz. Und die erfordert als allererstes solide Basis-Sicherheit quer durch alle Bereiche. Also Dinge wie Zweifaktor-Authentifizierung, Awareness und sichere Backups. Dass wir noch weit von guter Basis-Security entfernt sind, zeigt das organisierte Verbrechen, das mit recht simplen Ransomware-Angriffen Milliardenschäden anrichtet. Die überwiegende Mehrzahl dieser Cybercrime-Angriffe nutzt ganz triviale Versäumnisse bei der IT-Sicherheit.“ (Schmidt, 2022)

IT-Schutznahmen sind über viele Themen und Kompetenzfelder ausgeprägt. Der Grad des IT-Schutzes, den eine Organisation erreicht hat, kann mit Hilfe von Reifegradmodellen dargestellt werden. Folgende Ausführungen haben das Ziel, die Komplexität der Informationssicherheit zu verdeutlichen, um nachfolgend Vorschläge für sinnvolle Aktivitäten daraus abzuleiten.

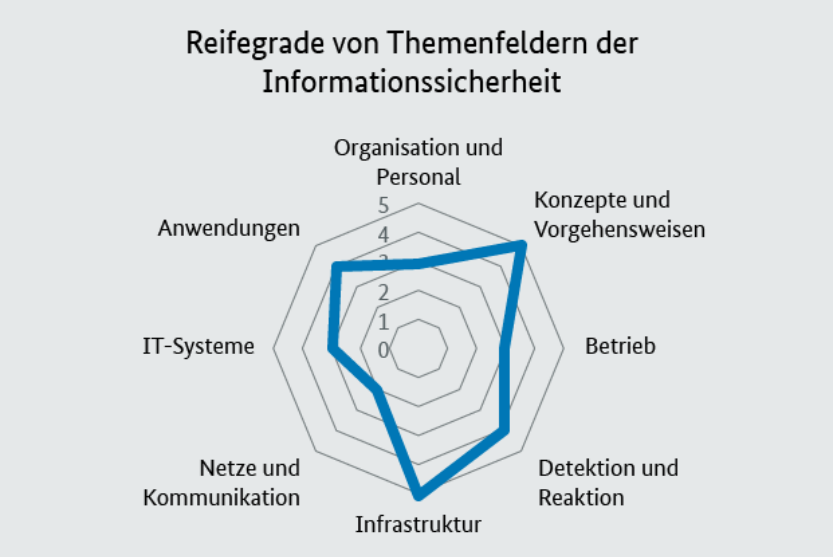


Abbildung 1: Reifegradmodell Informationssicherheit (BSI, 2022)

In *Abbildung 1: Reifegradmodell Informationssicherheit* ist zu erkennen, dass diverse Prozesse und Bereiche der IT-Infrastruktur einer Organisation betroffen ist. Nur ein strukturiertes Vorgehen kann eine hohe Maßnahmenqualität sichern. Die Wirksamkeit aller Maßnahmen bestimmt das Schutzpotential der Organisation. Dabei wird zwischen normativen und technischen Maßnahmen unterscheiden.

Aufgrund der Komplexität des Vorhabens IT-Sicherheit einer Organisation ist ein sogenanntes Informationssicherheitsmanagement zu verwenden, welches durch den Informationssicherheitsbeauftragen geführt wird. Diese zentrale Rolle wird auch in den „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik“ wie folgt beschrieben: „Es ist ein/e Informationssicherheitsbeauftragte/r (ISB) zu benennen. Diese/r soll außerhalb des operativen IT-Managements angesiedelt sein, um Interessen- und Rollenkonflikte zu vermeiden. Für ressortübergreifende, strategische Aufgaben der Planung und Steuerung des ISM ist ein/e Gesamtverantwortliche/r für die Informationssicherheit zu benennen.“ (Bundesrechnungshof, 2020)

Die IT-Sicherheitsanforderungen sind klar definiert. In den Kommunen finden wir größtenteils keine adäquate Umsetzung. Ursachen sind die gewachsenen IT-Strukturen und die moderate Sensibilisierung der Verwaltungsführungen. Neben der Eignung der ISB sind diese in den Organisationen auch mit formaler Macht und Ressourcen auszustatten, um die Veränderungsprozesse durchzuführen. *Abbildung 2: Verhältnis von Risikoreduktion und Kosten* zeigt, dass durch Einsatz von Ressourcen das Schutzniveau einer Organisation bis zu einem sinnvollen Maß erhöht werden kann. Die verbleibenden Restrisiken sind zu benennen, zu bewerten und eine Risikoübernahme ist zu autorisieren. Mit Hilfe des ISMS wird die Organisation befähigt, ein hohen IT-Sicherheitsschutz aufzubauen und ständig weiter zu entwickeln.

Die Herausforderungen liegen im Verhältnis der eingesetzten Ressourcen zu dem erreichten bzw. erreichbaren Schutzniveau.

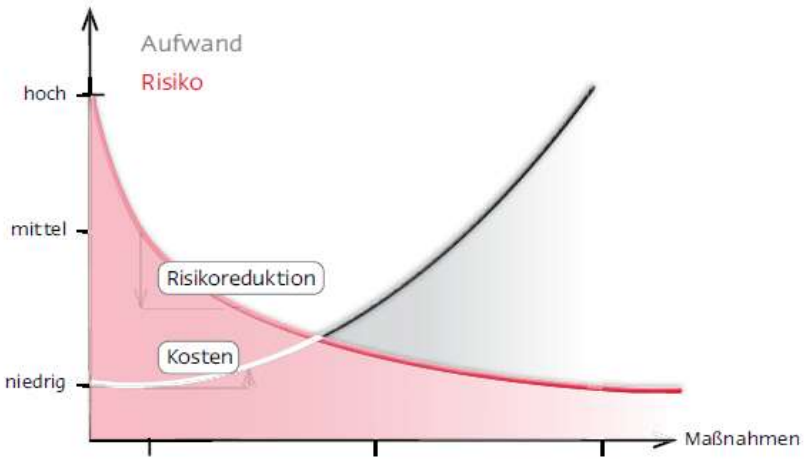


Abbildung 2: Verhältnis von Risikoreduktion und Kosten (Fox & u.A., 2019)

Entgegen der weit verbreiteten Meinung, dass IT-Sicherheit nur durch den Einsatz von speziellen IT-Systemen erreicht werden kann, ist durch eine prozessorientierte Vorgehensweise ein höherer Schutz zu erreichen. Dazu gilt es, die Geschäftsprozesse einer Organisation zu kennen und die in ihnen enthaltenen Risiken zu benennen und zu bewerten, da neben einem fachgerechten Einsatz der geschäftsprozessunterstützenden Systeme auch deren Sicherung und Wiederanlauf fixiert werden muss. Regelmäßige Tests der Sicherungsszenarien runden das Procedere ab. Den Umfang der notwendigen Maßnahmen zur Härtung der IT-Infrastruktur und der regelgerechten IT-Vorgehensweise zeigt die *Abbildung* 3: *Cybersecurity Reifegradmodell*.

Abbildung 3: Cybersecurity Reifegradmodell (Carsten Marmella, 09/2020)

Mit Hilfe einschlägiger Literatur lassen sich viele Maßnahmen ableiten. Es existieren dabei unterschiedliche Herangehensweisen. Eines haben alle gemein, den Schutzschild gegen Cyberangriffe stellen ein solides ISMS, unterstützt durch technische Sicherungsmaßnahmen mit oder ohne KI Unterstützung, sowie eine sensibilisierte und geschulte Belegschaft dar. Notfallpläne und Desaster-Recovery-Modelle ergänzen die Vorkehrungen hinsichtlich der Begrenzung der Folgen eines leider wahrscheinlichen, erfolgreichen Cyberangriffs.

Voranstehende Erläuterungen zeigen, dass Angriffspunkte bzgl. der IT-Sicherheit in den Organisationen zu finden sind. Somit müssen zwangsweise Maßnahmen zur Erhöhung dort ansetzen.

Durch das BSI[1] ist ein solides Rahmenwerk zur Sicherung der Organisationen gegeben. Mittels verschiedener ISO-Normen und Zertifizierungen besteht die Möglichkeit, gerade auch bei kritischen Infrastrukturen die eigenen IT-Prozesse zu bewerten bzw. bewerten zu lassen.

Die Banken und Sparkassen haben ein sehr hohes IT-Schutzniveau erreicht. Das liegt u.E. in

- der Sensibilisierung der Geschäftsführung durch das Bafin[2]
- der starken Prozessstandardisierung mit vorhandener Risikobewertung
- der Verwendung eines zertifizierten IT-Dienstleisters mit strikten Vorgaben
- den regelmäßigen behördlichen Kontrollen durch das Bafin
- den regelmäßigen in den Jahresabschluss integrierten IT-Audits
- den regelmäßigen Auditierungen des ISMS-Prozesses selbst
- der Bereitstellung von notwendigen finanziellen und personellen Ressourcen.

IT-Sicherheit kann durch ad hoc Maßnahmen gesteigert werden, sichere IT-Systeme in MV sind jedoch nur mittelfristig zu erreichen.

Ableitend aus den Darstellungen möchten wir Ihnen Vorschläge für Unterstützungsmaßnahmen zur Herstellung des erforderlichen IT-Sicherheitsreifegrads der kommunalen Institutionen des Landes MV sowie anderer Stakeholder übergeben.

[1] Bundesamt für Sicherheit in der Informationstechnik
[2] Bundesanstalt für Finanzdienstleistungsaufsicht

- Die Erarbeitung eines Informationssicherheitsförderungskonzeptes zusammen mit den Hoch- und Fachhochschulen des Landes MV
- Gründung und Leitung eines kommunalen IT-Sicherheitskompetenz – Teams MV ggf. über eGo-MV[3] mit den kommunalen ISB[4]
    - Berücksichtigung von Inhalten aus dem IT-Planungsrat[5]
    - Einbringen Inhalten aus dem CERT MV-Team[6]
    - Einbringen von Inhalten aus wissenschaftlichen Erkenntnisse
    - Einbringen von Ergebnissen aus (und ggf. Beteiligung an) Europäischen IT-Sicherheitsprojekten
- Unterstützung der Ausbildung der Menschen in MV
    - Forcierung der IT Ausbildung der Lehrkräfte für Lehrer an den Universitäten
    - Forcierung der IT Ausbildung von Lehrern
    - Erhöhung der Priorität der IT Ausbildung in den Schulen 2. Fremdsprache vs. Medienkompetenz der Schüler (z.B. Fach Informationstechnologie **nicht** Informatik)
    - Förderung von entsprechenden Veranstaltungen zur Sensibilisierung der Bevölkerung auch anhand praxisorientierter Workshops ggf. in den Volkshochschulen
- Befähigung des Landesrechnungshofes MV zur Durchführung qualitativer IT-Sicherheitsaudits in den Kommunen. Ggf. Übertragung der Aufgabe an den eGo-MV.
- Weitere Stärkung des CERT MV-Teams zur Erhöhung der proaktiven Handlungsfähigkeit
- Sensibilisierung der Kommunalen Führungen das Thema IT-Sicherheit stärker mit Vorgaben und Ressourcen zu unterstützen
- Förderung konsolidierter, kommunaler Rechenzentren
- Förderprogramm zur Unterstützung fortschrittlicher IT-Sicherheitsprojekte (KI – Einsatz)

Fazit:

Der Antrag der FDP mit den dargestellten Punkten entspricht u.E. nur zum Teil der benötigten Vorgehensweise zur Erhöhung des Reifegrades der IT-Sicherheit in MV, da er in großen Teilen auf den Bereich der Strafvereitelung und Strafverfolgung abzielt. Um die Strafverfolgungsbehörden nicht zu überlasten ist es dringend notwendig, den Schutz der Infrastruktur an sich zu erhöhen. In einer geschützten Infrastruktur gelingen Cyberangriffe dennoch, diese können dann effektiver und erfolgreicher nachverfolgt werden.

Die Forderung der FDP im Punkt 2 *(„IT-Studiengänge voranzutreiben")* ist u.E. nachvollziehbar und wird von uns uneingeschränkt mitgetragen. Insbesondere, da es auch den Kommunen aktuell sehr schwer gelingt, ausgebildete Fachkräfte zu akquirieren. Selbst ausgebildetes Personal wird aufgrund von Marktverschiebungen[7] durch diesen

[3] Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern
[4] Informationssicherheitsbeauftragten
[5] Der IT-Planungsrat fungiert als zentrales politisches Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen
[6] Computer Emergency Response Team - In einem **CERT** arbeiten IT-Spezialisten und Sicherheitsfachleute an der Lösung von konkreten Sicherheitsvorfällen
[7] Für Mitarbeiter im Bereich der Informations- und IT-Sicherheit werden hohe Gehälter geboten

Fachkräftemangel abgeworben. Neben der Bereitstellung von Personal für die Dienststellen des Landes würden bei entsprechender Ausprägung der Programme sowohl die Kommunen als auch die Wirtschaft des Landes MV davon partizipieren. Die Dringlichkeit des Bedarfes wurde bereits in den weiteren Abschnitten dieser Stellungnahme unterstrichen.

Zu Punkt 4 *(„Cybercrime Dienststellen ... besser ausstatten“*) möchten wir nicht Stellung beziehen, da uns hier die notwendigen Informationen bzgl. der aktuellen Ausstattung und Rahmenbedingungen fehlen. Ebenso fällt uns eine Stellungnahme zu den Punkten 1 und 3 schwer, da hier u.E. nicht erklärt wird, wofür das gut ausgebildete IT-Personal in den Dienststellen verwendet werden soll. Die Forderung korreliert jedoch mit unserem Vorschlag, den Rechnungshof mit qualifizierten Mitarbeitern auszustatten, um die Kommunen in MV bei der Schaffung geregelter IT-Sicherheitsprozesse zu unterstützen. Alternativ könnte auch dem eGo-MV diese Aufgabe übertragen werden.

Zusammenfassend erscheint es sinnvoll, auch in Vorgehensweisen zu investieren, die eine breite Wirkung bei der Verbesserung der Informationssicherheit bewirken.

Die durch die Corona-Pandemie und dem Ukrainekrieg verschärften Rahmenbedingungen der sicherheitsrelevanten IT-Anwendungen hat den Senior Fellow Security bei Heise, Jürgen Schmidt bewogen, folgenden Aufruf zu verfassen.

„Was wir jetzt also brauchen, ist ein Ruck, hin zu mehr IT-Sicherheit, der quer durch die ganze Gesellschaft geht! Deshalb appelliere ich an:

- Politiker: IT-Sicherheit schafft keine neuen Umsätze und spart keine Ausgaben ein – im Gegenteil. Wir brauchen deshalb dringend "Anreize" zur Verbesserung der IT-Sicherheit auf allen Ebenen.

- IT- und Sicherheits-Verantwortliche in Unternehmen und Behörden: Ihr wisst in aller Regel, woran es fehlt. Erklärt euren Vorgesetzten, dass dieser Krieg die Prioritäten ändert. IT-Sicherheit ist nicht mehr "nice to have", sondern tatsächlich überlebenswichtig – ihr seid kritische Infrastruktur. Zeigt ihnen, welche Maßnahmen jetzt aus eurer Sicht kurz- und mittelfristig anzugehen sind.

- Anwender: Achtet auf Sicherheit –, auch wenn es manchmal etwas unbequemer ist.“ (Schmidt, 2022)

Rostock, 23.03.2022

Sven Bradtke
i.A. Amtsleiter
Amt für Digitalisierung und IT
Hanse- und Universitätsstadt Rostock

Abbildungsverzeichnis

Literaturverzeichnis

BSI. (2022). *Online-Kurs IT-Grundschutz*. Von Lerneinheit 9.4: Reifegradmodelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_9_Aufrechterhaltung/Lektion_9_04/Lektion_9_04_node. abgerufen

Bundesrechnungshof. (2020). *Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik.*

Carsten Marmella. (09/2020). *Cybersecurity Reifegradmodell.* carmasec GmbH und CoKG.

Fox, D., & u.A. (2019). *Informationssicherheit und Datenschutz.* Heidelberg: dpunkt.verlag GmbH.

Schmidt, J. (23. 03 2022). *Heise.* Von Kommentar zum Ukraine-Krieg: Wo bleiben die Milliarden für IT-Sicherheit? : https://www.heise.de/meinung/Kommentar-zu-Russlands-Krieg-Wo-bleiben-die-Milliarden-fuer-IT-Sicherheit-6611781.html abgerufen

SIS – Schweriner IT- und Servicegesellschaft mbH, Eckdrift 93, 19061 Schwerin

Landtag
Mecklenburg-Vorpommern
Ausschuss für Inneres, Bau
und Digitalisierung
-Der Vorsitzende-
Lennéstraße 1 (Schloss)
19053 Schwerin

Bearbeiter: Marco Block
Tel.: 0385 -545-5201
Fax: 0385 633-5109
Mail: marco.block@sis-schwerin.de

Ihr Zeichen:
Unser Zeichen: 02-4-06

Datum: 23.03.2022

Per E-Mail: innenausschuss@landtag-mv.de

Stellungnahme zum Antrag der Fraktion der FDP – „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen“

Sehr geehrter Herr Vorsitzender Mucha,
Sehr geehrte Damen und Herren,

zur Vorbereitung der Sitzung am Donnerstag, den 31. März 2022 senden wir Ihnen vorab unsere schriftlichen Ausführungen zum Antrag der Fraktion der FDP.

A. Kurzvorstellung des Unternehmensverbundes
Der Unternehmensverbund SIS/KSM ist der zentrale kommunale Full-Service-IT-Dienstleister im Westteil des Landes Mecklenburg-Vorpommern. 2006 mit zunächst knapp 50 Beschäftigten der Landeshauptstadt Schwerin und ihrer kommunalen Unternehmen gestartet, betreuen knapp 250 Beschäftigte heute als Full-Service-IT-Dienstleister die Landeshauptstadt Schwerin, den Landkreis Ludwigslust-Parchim sowie weitere 11 Städte und Ämter im Landkreis, einen signifikanten Anteil deren kommunaler Unternehmen sowie deren Schul-IT. Der Unternehmensverbund betreibt am Standort Schwerin ein eigenes Rechenzentrum, über das regelmäßig die Bereitstellung der Leistungen für die Kunden und Träger erfolgt. Außerhalb des Standortes in Schwerin sind wir mit eigenen Servicepoints in Ludwigslust, Parchim, Boizenburg, Zarrentin und Wittenburg präsent.

B. Stellungnahme zu den im Antrag benannten Themen
Wenn man die derzeitige Lage unter Personalgesichtspunkten betrachtet, ist festzustellen, dass an wichtigen Stellen ein Defizit besteht. Wichtige Positionen wie bei der Administration von Sicherheitssystemen, Firewalls oder auch Erkennungssystemen (IDS/IPS) sind unterbesetzt und zusätzliche bzw. freiwerdende Stellen können nur mit sehr großen Aufwand besetzt werden.

Als langjährig ausbildendes Unternehmen ist die SIS seit Anfang an bestrebt, ihre Auszubildenden mit den nötigen Kompetenzen

SIS – Schweriner IT- und Servicegesellschaft mbH
19061 Schwerin
Eckdrift 93
Tel.: 0385 633-5100
Fax: 0385 633-5109
Mail: info@sis-schwerin.de

Bank:
Sparkasse Mecklenburg-Schwerin
IBAN: DE12 1405 2000 1613 0017 9
BIC: NOLADE21LWL

Sitz der Gesellschaft:
Schwerin
Amtsgericht Schwerin
HRB-Nr. 8855
Steuernr. 079/133/31464

Vorsitzender des Aufsichtsrates
Bernd Schulte

Geschäftsführer
Matthias Effenberger

auszustatten. In den letzten Ausbildungsjahren ist vermehrt festzustellen, dass durch die Berufsschulen die nötige Basiskompetenz bei bspw. Fachinformatikern nicht mehr aufgebaut werden kann. Gründe dafür sind fehlende Lehrkräfte und bedingt dadurch der Ausfall von wichtigen Lehrinhalten, welche auch nicht mehr nachgeholt werden bzw. werden können. Sofern dies überhaupt möglich ist, muss dieser Mangel dann mühsam durch die Ausbildungsbetriebe aufgefangen werden. Fehlende örtliche Weiterbildungsmöglichkeiten spielen dahingehend auch eine große Rolle.

Auch mit den Hochschulen des Landes gibt es eine intensive Zusammenarbeit, sei es über die Bereitstellung von Plätzen für Praktika oder über unsere Studenten in dualen Studiengängen.
Eine „Kannibalisierung" der kommunalen IT-Strukturen durch verstärkte Personalnachfragen des Landes ist kontraproduktiv. Vielmehr sind alle öffentlichen IT-Beteiligten im Land gefordert, ihre Aus- und Fortbildungsbemühungen zu intensivieren.
Eine Weiterentwicklung der IT-Studiengänge im Land, besonders unter dem Focus Cyper- bzw. Informationssicherheit wäre zu begrüßen. Nach Wahrnehmung der aktuellen Situation gibt es im Land keine etablierten Strukturen, die die Weiterbildung hinsichtlich Sensibilisierung und Qualifizierung in Bezug auf IT-Sicherheit organisiert. Auf der kommunalen Ebene sind es in der Regel die kommunalen IT-Dienstleister und Aufgabenträger, wie SIS, KSM und IKT-Ost und auch der Zweckverband Elektronische Verwaltung.
Eine finanzielle Unterstützung des Landes, zumindest in Form einer Anschubfinanzierung, für die Bildung von Security Operation Centern (SOC's) bei den kommunalen IT-Dienstleistern mit eigenen RZ-Kapazitäten wäre angesichts der stetig steigenden Bedrohungslage sicher sehr wünschenswert. Durch ein abzustimmendes Betriebsregime der Center könnten gut ausgebildete IT-Experten zu jedem Zeitpunkt verfügbar sein und dies in der Regel 24/7 an 365 Tagen. Diese SOC`s könnten darüber hinaus auch als permanente Ansprechpartner für das CERT MV fungieren.

C. Ergänzende Anmerkungen und Empfehlungen
Cyberangriffe auch auf Kommunalverwaltungen sind nach unserer Ansicht und vieler Sicherheitsexperten, sowie auch kommunaler Spitzenverbände, ein wiederkehrendes Problem. Eine hundertprozentige Sicherheit ist nicht herzustellen, einen Angriff kann es überall geben. Es ist sowohl weltweit als auch deutschlandweit zu beobachten, dass versucht werde, Kommunalverwaltungen oder auch kommunale Einrichtungen – wie etwa Stadtwerke - anzugreifen. Entscheidend ist, dass die IT-Systeme und damit auch die Sicherheit in den Verwaltungen ständig weiterentwickelt würden.

An Professionalität zunehmende Angriffe stellen die Verantwortlichen vor große Herausforderungen, gerade wenn man gewohnte Umgebungen und sichere Strukturen verlassen muss. Einmal ein Sicherheitskonzept zu erstellen, reicht nicht aus. Cybersicherheit ist ein kontinuierlicher Prozess und muss stets an die Rahmenbedingungen angepasst werden.

Inwieweit zwischen Land und Kommunen abgestimmte, zusätzliche Vergütungsanreize dem Fachkräftemangel ein Stück entgegenwirken könnten wäre zu untersuchen.

Bei Rückfragen stehen wir Ihnen jederzeit gern zur Verfügung.

Freundliche Grüße

SIS – Schweriner IT- und Servicegesellschaft mbH

Matthias Effenberger
Geschäftsführer

Gerhard Lienau
Prokurist

Bund Deutscher
Kriminalbeamter
Mecklenburg-Vorpommern

BDK M-V | Ulmenstraße 54 | D-18057 Rostock

An
die Mitglieder des Ausschusses für Inneres,
Bau und Digitalisierung

per Mail: innenausschuss@landtag-mv.de

Landesvorstand

Ansprechpartner/in: Stephan Gäfke
Funktion: Bezirksvorsitzender Schwerin

E-Mail: stephan.gaefke@bdk.de
Telefon: +49 auf Anfrage

Datum: 24.03.2022

ANTRAG der Fraktion der FDP
Cyber-Kriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen

Stellungnahme des Bund Deutscher Kriminalbeamter Mecklenburg-Vorpommern

Sehr geehrte Damen und Herren,

zunächst bedanken wir uns recht herzlich für die Möglichkeit der Stellungnahme. Der Bund Deutscher Kriminalbeamter (BDK) M-V begrüßt grundsätzlich die Aufforderungen an die Landesregierung zu den Punkten 1-5.

Der BDK M-V hat dazu nachfolgende Anmerkungen:

Punkt 1: Die Landesregierung wird aufgefordert, mehr gut ausgebildetes Personal für den Bereich IT-Sicherheit und Infrastruktur bereitzustellen.

Struktur und Rolle der Kriminalpolizei M-V
Einleitend soll die Struktur und Rolle der Kriminalpolizei in Bezug auf IT-Sicherheit und Infrastruktur sowie der Cybercrime-Bekämpfung dargelegt werden.

Grundlegend geht es bei Cybercrime nach unserer Auffassung um digitale Kriminalitätserscheinungen jeglicher Art. Sei es die Beleidigung über WhatsApp, die Erpressung per E-Mail oder die Verschlüsselung von Firmendaten aus der Ferne durch Cyberkriminelle.

Cybercrime ist mehr als Angriffe auf kritische Infrastrukturen.

Polizeilich unterscheidet man zwischen „Cybercrime im engeren Sinne“ (Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten) und „Cybercrime im weiteren Sinne“ (Straftaten, die mittels Informationstechnik begangen werden). Cybercrime im weiteren Sinne stellt vereinfacht gesagt, Taten dar, die auch in der

analogen Welt begangen werden können, wie etwa der Drogenhandel oder die Beleidigung. Cybercrime im engeren Sinne sind hochtechnische Straftaten, die ebensolche hochtechnische Ermittlungsarbeit auf Seiten der Polizei erfordern. Cybercrime ist ein hochkomplexer, krimineller Wirtschaftszweig mit eigenen Wertschöpfungsketten und arbeitsteiligem Vorgehen.[1]

Dementsprechend werden die Straftaten den (qualifizierten) Kriminalpolizeidienststellen zur Bearbeitung zugewiesen. Nicht selten kommt es schon hierbei zu falschen Kategorisierungen der Delikte durch die aufnehmenden Beamten, so dass sich die Bearbeitung der Vorgänge verzögert. Im Extremfall findet ein „Vorgangs-Ping-Pong“ statt, da Diskussionen über die sachliche Zuständigkeit zwischen den Kriminalpolizeiinspektionen (KPIen) und den Kriminalkommissariaten (KKen) stattfinden.

Der Großteil der Cybercrimedelikte (Cybercrime im weiteren Sinne) wird in den 8 Kriminalkommissariaten in M-V bearbeitet. Daneben bearbeiten die Kriminalpolizeiinspektionen und das LKA Cybercrimedelikte, wenn hochtechnische Ermittlungsarbeit notwendig ist.

Akteure der IT-Sicherheit und Infrastruktur in M-V

Einen klaren abgrenzbaren Bereich „IT-Sicherheit und Infrastruktur“ gibt es in der Regierungsstruktur in Mecklenburg-Vorpommern nicht. Deutschlands staatliche Cybersicherheitsarchitektur insgesamt ist in Gänze schwer durchschaubar und sehr komplex.[2]

Die im Folgenden beispielhaft aufgelisteten Akteure aus M-V nehmen unterschiedliche Aufgaben auf den Feldern der IT-Sicherheit und Infrastruktur wahr:

- Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ) GmbH[3]
- Landesamt für Zentrale Aufgaben und Technik der Polizei, Brand und Katastrophenschutz (LPBK)[4]
- Computer Emergency Response Team M-V (CERT M-V)[5]
- Koordinierungsstelle KRITIS (KOST KRITIS, IM M-V)
- IT-Sicherheitsbeauftragte der Landesbehörden

Das DVZ hat eine Vielzahl von Geschäftsfeldern (z. B. IT-Forensik, Entwicklung von Fachverfahren, Betrieb eines Hochsicherheits-Rechenzentrums) und ist IT-Dienstleister des Landes M-V.

Für die IT-Sicherheit und Infrastruktur innerhalb der Landespolizei M-V ist u.a. das LPBK zuständig.

Seit 2. Februar 2015 sorgen die Spezialisten des CERT M-V für die IT-Sicherheit in den kommunalen und staatlichen Stellen des Landes.

Die Aufgaben der KOST KRITIS werden im unteren Teil näher erörtert.

[1] https://www.bka.de/DE/KarriereBeruf/ArbeitenBeimBKA/Einblicke/Cybercrime/cybercrime_node.html
[2] https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur#collapse-newsletter_banner_bottom
[3] https://www.dvz-mv.de/
[4] https://www.polizei.mvnet.de/Polizei/LPBK-MV/
[5] https://www.regierung-mv.de/Landesregierung/im/Digitalisierung/informationssicherheit/informationssicherheit-in-der-verwaltung/

Aufgabe der Kriminalpolizei M-V

Die Aufgabe der Kriminalpolizei in M-V besteht nicht darin unmittelbar für IT-Sicherheit zu sorgen und sich um die IT-Infrastruktur zu kümmern. Die Kriminalpolizei hat die gesetzliche Aufgabe Straftaten zu verfolgen und Gefahren abzuwehren.[6] Für IT-Sicherheit sorgt die Kriminalpolizei daher maximal im Rahmen von persönlichen bzw. telefonischen Beratungen oder Vorträgen von Unternehmen durch die Zentrale Ansprechstelle Cybercrime (ZAC M-V) oder durch andere Polizeidienststellen mit Bürger- und Unternehmenskontakt. Die ZAC M-V ist im Landeskriminalamt (LKA M-V)[7] angesiedelt.

Bundesamt für Sicherheit in der Informationstechnik

Eine besondere Bedeutung hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), welches die Aufgabe hat, die Sicherheit in der Informationstechnik des Bundes zu stärken und die präventive Informations- und Cyber-Sicherheit zu fördern, um den sicheren Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft zu ermöglichen und voranzutreiben.[8]

Cybercrime-Strategie 2014 und Entwicklung danach

Seit der Erstellung der Cybercrime-Strategie für die Landespolizei M-V durch das LKA M-V im Jahr 2014 konnten viele Fachkräfte für das LKA, LPBK und die 4 Kriminalpolizeiinspektionen als Seiteneinsteiger (IT-Master bzw. IT-Bachelor gem. §16 PolLaufbVO M-V[9]) gewonnen werden. Das war ein wichtiger Schritt und hat die Landespolizei als Ganzes vorangebracht. Dieser Weg muss aus unserer Sicht verstärkt werden, weil noch in vielen Ermittlungsbereichen außerhalb von Cybercrime notwendiges IT-Know-How fehlt.

Vergessen werden darf hierbei nicht, dass in der Landespolizei im Jahr 2021 insgesamt 318 Polizeivollzugsdienststellen nicht besetzt waren und ohnehin Personal an vielen Stellen fehlt.[10]

Das Land M-V steht in unmittelbarer starker Konkurrenz zur Region Hamburg und Berlin, wo deutlich höhere Einkommen im privaten IT-Sektor für Arbeitnehmer:innen zu erzielen sind. Das erschwerte die Fachkräftegewinnung in M-V in den letzten Jahren wesentlich. Zu öffentlichen Stellenausschreibungen der Landespolizei M-V war in der nahen Vergangenheit nicht die notwendige Anzahl an Bewerber:innen und das entsprechende Niveau an IT-Expertise zu verzeichnen.

[6] https://www.gesetze-im-internet.de/stpo/__163.html
https://www.landesrecht-mv.de/bsmv/document/jlr-SOGMV2020pG2
[7] https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
[8] https://www.bsi.bund.de/DE/Service-Navi/FAQ/BSI-Aufgaben/faq_bsi-aufgaben_node.html
[9] https://www.landesrecht-mv.de/bsmv/document/jlr-PolLbVMV2011V1P16
[10] https://www.dokumentation.landtag-mv.de/parldok/dokument/51597/ueberstunden_bei_der_landespolizei_in_mecklenburg_vorpommern.pdf, Bl. 4

Bereits gewonnenes IT-Fachpersonal innerhalb der Kriminalpolizei muss bei Laune gehalten werden, um es zu halten. Ansonsten wandert es zu den Arbeitgeber:innen ab, die nicht nur finanziell bessere Bedingungen bieten. Es geht neben dem finanziellen Aspekt, die nicht unwichtig sind, auch um

- Selbstverwirklichung des IT-Fachpersonals
- Wertschätzung durch Führungskräfte
- und einer sinnhaften motivierenden Tätigkeit.

Wenn Behörden in der Landespolizei Selbstverwirklichung nicht zulassen und bei guten Ideen immer wieder den Riegel vorschieben, verlassen die IT-Expert:innen die Landespolizei und suchen sich eine bessere Alternative. Offene lukrative Stellen auf dem Arbeitsmarkt sind ausreichend vorhanden.

In der alltäglichen Praxis sehen sich IT-Fachkräfte in der Kriminalpolizei viel zu oft mit zu vielen parallel laufenden Projekten konfrontiert, die zum „Papiertiger“ mutieren und bei denen am Ende nur eine Kompromisslösung herauskommt, ohne wirklich was erreicht zu haben. Unmittelbar spürbare Arbeitserleichterung entfalten IT-Projekte in der Landespolizei M-V nur selten.

Oft spielen die Finanzen, vielfache Abhängigkeiten und lähmende Bürokratie bei der Realisierung von IT-Projekten eine gewichtige Rolle. Das demotiviert IT-Fachkräfte, weil sie ihrer eigentlichen Aufgabe nicht mehr nachgehen können und stattdessen in sinnlos erscheinenden Projekten gebunden werden. Teilweise wird die tatsächliche Arbeit als stupide und wenig herausfordernd gesehen. Es werden zum Teil „Perlen vor die Säue“ geworfen. Hinzu kommen artfremde Verwendungen von IT-Fachkräften. Die eigentlich vorgesehenen Aufgaben können nicht mehr erledigt werden. Das führt zu Frust.

Das Motto sollte lauten: „Weniger Konzepte, weniger reden und mehr machen.“

Ebenso problematisch ist, dass langwierige und kostenintensiv erarbeitete Konzeptpapiere zu oft in den Schubladen verschwinden, weil sie am Ende nicht finanziert werden können.

Gute Ideen und Vorschläge von IT-Fachkräften werden von unmittelbaren Vorgesetzten nicht aufgegriffen, weil man u.a. Bedenken und teilweise Angst vor Investitionen (Personal, Zeit und Geld) hat.

Um mehr gut ausgebildetes Personal für die Kriminalpolizei in M-V zu gewinnen, sind aus unserer Sicht folgende Faktoren ausschlaggebend:

- berufliche Aufstiegschancen für IT-Fachkräfte
- angemessene Eingruppierung der IT-Fachkräfte
- Gewährung einer IT-Fachkräftezulage (siehe IT-Prämie im Bund)
- Ermöglichung des Laufbahnaufstiegs in den höheren Dienst (z.B. für IT-Masterabsolventen)
- Freiräume für Fachkräfte zur beruflichen Weiterqualifizierung (Nebentätigkeiten, weiteres Studium, Weiterbildung, etc.)
- Freiräume für ein Sabbatjahr um sich beruflich zu qualifizieren

- weniger parallel laufende IT-Projekte im beruflichen Alltag
- stellenbezogene Aufgabenwahrnehmung
- Ausschöpfung der Höhergruppierung von Angestellten wenn dies gesetzlich möglich ist

In der Führungsebene wird der intrinsisch motivierte Wille der Mitarbeiter:innen in der Landespolizei für ein weiterführendes Studium oder eine andere berufliche Weiterqualifizierung nicht selten als Privatvergnügen der Mitarbeiter:innen angesehen, obwohl die Landespolizei von diesen Qualifizierungen auch profitiert. Fachlichkeit fällt nicht vom Himmel und braucht Raum zur Entwicklung.
Sind die o.g. Faktoren nicht gegeben, kam es in der Vergangenheit zu Personalfluktuation und u.a. zum Verlassen der Landespolizei M-V in andere Bundesländer bzw. zu anderen Arbeitgebern (Finanzamt, Hochschulen, Privatunternehmen, etc.) aufgrund höherer Besoldung oder besserer beruflicher Perspektiven. Natürlich spielen auch private Aspekte eine gewichtige Rolle. Zur Personalabwanderung wird es bei Beibehaltung der ungünstigen Umstände innerhalb der Landespolizei auch in Zukunft kommen. Das muss unbedingt vermieden werden.

Die Personalfluktuation schwächt die Landespolizei außerordentlich, da Erfahrungswissen und Kompetenzen unmittelbar verloren gehen. Erfahrungswissen wird in Behörden immer noch schlecht konserviert und bleibt zu oft in den Köpfen der abwandernden (auch pensionierten) Mitarbeiter:innen. Die Landespolizei muss dadurch an vielen Stellen immer wieder von vorne anfangen und vergeudet hierfür zu viel Zeit.

Punkt 2: Die Landesregierung wird aufgefordert, gemeinsam mit den Hochschulen des Landes ein Konzept zu entwickeln, die Weiterentwicklung der IT-Studiengänge voranzutreiben sowie entsprechende Stipendienprogramme aufzulegen.

Seit Jahren gibt es eine Hochschulkooperation mit der Hochschule in Wismar[11] und Rostock[12]. Diverse IT-Absolvent:innen der Hochschule Wismar wurden in der Vergangenheit bei ihrer Masterarbeit vom LKA M-V betreut und konnten im Anschluss für die Kriminalpolizei M-V gewonnen werden. Das war richtig und wichtig.

Eine Hochschulkooperation mit der Hochschule Stralsund ist uns nicht bekannt und sollte schnellstens mit dem LKA vereinbart werden, da auch in Stralsund IT-Fachkräfte für die Zukunft gewonnen und in M-V gehalten werden können. Wer in M-V Wurzeln und in Stralsund studiert hat, bleibt eher hier und wandert nicht in andere Bundesländer ab.

Es existiert neben den Hochschulkooperationen eine Arbeitsgemeinschaft (AG) Hochschulkooperation im LKA mit dem Ziel, sich besser mit Hochschulen und anderen Akteuren der Fachkräftegewinnung zu vernetzen und in der Öffentlichkeit zu präsentieren.

18 IT-Nachwuchskräfte wurden 2019 für die Landespolizei angestellt und absolvieren ein duales IT-Studium an den Hochschulen Wismar und Stralsund oder an der Universität Rostock. In der vorlesungsfreien Zeit werden Praktika bei der Landespolizei wahrgenommen.[13] Das ist ein gangbarer Weg um die Polizeiarbeit kennenzulernen und IT-Wissen und Polizeiarbeit

[11] https://www.wings.hs-wismar.de/de/presse/wings_partner1
[12] https://www.emerge-iot.de/
[13] https://www.presseportal.de/blaulicht/pm/108531/4388892

miteinander zu vernetzen. Leider sind von den 18 Studenten nicht mehr alle dabei. Solche Programme sind gut und sollten beibehalten werden. Eine Wirkung entfalten diese Programme jedoch erst verzögert, wenn das Studium abgeschlossen und Berufserfahrung aufgebaut ist. Momentan durchlaufen die IT-Studierenden viele Stationen in der Kriminalpolizei (Cybercrime, IT-Forensik, Telekommunikationsüberwachung, IT-Grundsatz im LKA, LPBK, KPIen) um viele Bereiche der Landespolizei kennenzulernen. Während des Studiums sollten die Studierenden mit der Durchführung von langfristigen Praktika und Ausarbeitung von kleinen Projekten schon an ihre präferierte Station gebunden werden um sie dort auch langfristig zu binden.

Man muss JETZT(!) an die Hochschulen herantreten und Masterarbeitsthemen platzieren umso Personal für die Landespolizei zu gewinnen. Dafür braucht es geeignete Betreuer:innen in der Kriminalpolizei. Vorgesetzte müssen hier an einem Strang ziehen und auch wollen, dass „eigenes“ Personal der Kriminalpolizei bei der Masterarbeit eine Betreuung durchführt. Diese Aufgabe der Betreuung von Bachelor- und Masterarbeiten muss auch in der Stellenbeschreibung des durchführenden Personals aufgenommen werden, damit diese Aufgabe rechtlich gebunden und geregelt ist und nicht erst darum gerungen werden muss.

Punkt 3: Die Landesregierung wird aufgefordert, Strategien zu entwickeln, um Angriffe besser zu vereiteln und die Täter zu identifizieren, zu verfolgen und zur Rechenschaft zu ziehen.

Die Kriminalpolizei sieht sich täglich einer sehr dynamisch verändernden IT-Welt gegenüber und muss sich an die Lage immer wieder neu anpassen und ausrichten. Das war so und wird immer so bleiben. Täter passen sich immer neuen IT-Präventionsstrategien an und richten ihr Handeln dementsprechend aus. Softwareschwachstellen bei Unternehmen werden gnadenlos und zum eigenen finanziellen Vorteil von Cyberkriminellen ausgenutzt.

Die Pandemiesituation hat seit März 2020 definitiv dazu beigetragen, dass die digitalen „Fenster und Türen“ in Unternehmen offener stehen und anfälliger sind. Dazu trägt zum einen bei, dass Mitarbeiter:innen aus dem Home-Office auf Unternehmensnetzwerke zugreifen müssen. Zum anderen tragen bekannte als auch noch unbekannte Softwareschwachstellen in Kombination mit automatisierten Angriffstools dazu bei, dass Cyberangriffe in kürzeren Abständen und häufiger stattfinden können.

Des Weiteren tragen Entwicklungen wie die Ausbreitung von Smart-Home-Geräten im geschäftlichen und privaten Umfeld dazu bei, dass sich digitale Angriffspunkte vermehren und immer mehr Geräte miteinander vernetzt sind. Weniger Smart-Home wäre mehr IT Sicherheit.

Asymmetrie zwischen Staat und Kriminellen
Die Kriminalpolizei handelt nach den gesetzlichen Regelungen in Deutschland und der EU. Cyberkriminelle agieren weltweit und handeln wie sie wollen. Oft nutzen sie geopolitische Konflikte zu ihrem Vorteil, um nicht zur Rechenschaft gezogen zu werden. Diese starke Asymmetrie zwischen Staat und Kriminellen besteht schon seit Jahrzehnten und erschwert die Ermittlungstätigkeit – nicht nur im Bereich Cybercrime.

Gute Strategien um Angriffe besser zu vereiteln muss die Landesregierung sich nicht neu ausdenken. Es gibt sie bereits, z. B. beim BMI[14], BSI[15] oder auch in den USA[16].

Internationale polizeiliche Zusammenarbeit
Ein Schlüssel um Täter zur Rechenschaft zu ziehen, ist die verstärkte internationale polizeiliche Zusammenarbeit und der dazugehörige Informationsaustausch. Dieser Teil muss auf politischer Ebene noch viel stärker kommuniziert und ausgebaut werden, um gesetzliche und technische Hürden für die Strafverfolgung abzubauen. Daten sind der zentrale Baustein, um Täter zu identifizieren und lokalisieren.

Ein weiterer Punkt könnte unter Beachtung des Trennungsgebotes der generelle Informationsaustausch mit Nachrichtendiensten (LfV, BfV, BND) sein. In M-V findet ein solcher im Cybercrimebereich kaum bis gar nicht statt.

Cybercrime-Strategie
Das LKA M-V hat 2014 eine Cybercrime-Strategie entwickelt und Handlungserfordernisse formuliert. Diese wurden bis heute teilweise umgesetzt. Im Jahr 2019/2020 wurde das Konzept evaluiert. Ein Ergebnis liegt uns nicht vor. Nun wird es Zeit dieses Konzept vollständig umzusetzen. Oftmals scheitern Umsetzungen leider an fehlendem Geld. Als Beispiel sei hier das Projekt „Massendateninfrastruktur für die Landespolizei“ genannt. Das Konzeptpapier war fertig und die Ideen gut. Jedoch fehlten sowohl Geld als auch das qualifizierte Personal, um das Projekt vollständig mit allen Aspekten umzusetzen. Vielleicht fehlte auch der Wille im LPBK ein noch weiteres Großprojekt an Land zu ziehen. Stattdessen werden Insellösungen für die Auswertung von Asservaten in den Dienststellen geschaffen und ein organisatorischer Wildwuchs entsteht.

Ein weiterer wichtiger Baustein ist die ausreichende Ausstattung mit Soft- und Hardware in allen Cybercrime-Dienststellen und nicht nur im LKA und in den KPIen. Noch längst nicht alle Ermittler:innen in den Kriminalkommissariaten haben einen eigenen Internetrechner, um Recherchen zu tätigen oder Daten in angemessener Zeit auszuwerten.

[14] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf
[15] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
[16] https://www.golem.de/news/security-bei-der-us-regierung-vpn-sms-codes-und-passwoerter-sind-out-zero-trust-ist-in-2202-162871.html
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Aus- und Fortbildung an der FHöVPR Güstrow

In der Cybercrime-Strategie aus 2014 wurde auch die Aus- und Fortbildung für Cybercrime-Ermittler:innen beleuchtet. Wiedermal sind die Ideen gut und das Konzept steht. Nur wer soll es umsetzen? Das beste Konzeptpapier nützt nichts, wenn man es nicht mit Leben erfüllen kann. So kam es, dass das Aus- und Fortbildungskonzept in der FHöVPR Güstrow nicht vollständig umgesetzt werden kann. Die Gründe sind vielfältig und lassen sich wie folgt zusammenfassen:

- nicht genug Lehrpersonal vorhanden
- geringe Anzahl von entsendeten Mitarbeiter:innen aus Dienststellen
- zu viele Auszubildende/Studierende, die vorrangig ausgebildet werden müssen
- Ausbildung geht vor Fortbildung
- zu viele Aufgaben neben der eigentlichen Lehrtätigkeit an der FHöVPR
- Lehrkräfte sind teilweise auf Abordnungsbasis an der FHöVPR und müssen ständig neu angelernt werden

Punkt 4: Die Landesregierung wird aufgefordert, Cybercrime-Dienststellen in den Behörden des Landes besser auszustatten und landesweit zu koordinieren.

Die technische Ausstattung von Cybercrime-Dienststellen in der Kriminalpolizei M-V weist große Unterschiede zwischen LKA/KPI und den KKen auf. Die technische Ausstattung der Dienststellen wurde in der Cybercrime-Strategie 2014 in Anlagen definiert.

Die Cybercrime-Dienststellen des LKA und der KPIen sind verhältnismäßig gut ausgestattet. Andere Ermittlungsbereiche des LKA/der KPIen haben wie bereits oben erwähnt teilweise keinen personengebundenen Internetrechner für Recherchen und Auswertungen.

Die KKen sind teilweise auch schon nach der definierten Anlage aus der Cybercrime-Strategie 2014 ausgestattet. Hier gibt es jedoch regionale Unterschiede und auch hier haben längst nicht alle Ermittler:innen einen personengebundenen Internetrechner für die alltägliche Ermittlungsarbeit. Teilweise müssen in den KKen Anträge für die Nutzung von Standardsoftware (Firefox/Thunderbird) auf Internetrechnern geschrieben werden und wertvolle Zeit damit verschwenden. Aus unserer Sicht ein unhaltbarer Zustand.

Aus Führungskreisen wird immer wieder eine virtualisierte Internetlösung im Polizeinetz (LISA3) als Lösung angebracht, die jedoch nicht praktikabel ist und die aktuellen Anforderungen an Internetermittlungen und Recherchen nicht erfüllen kann.

Vorschläge aus Ermittlerkreisen für eine landesweite Umgebung von virtuellen Servern um damit Recherchen und Ermittlungen durchführen zu können, werden von Vorgesetzten teilweise nicht aufgegriffen. Es wird nicht mal Stellung dazu genommen, obwohl diese landesweite Umgebung eine große Wirkung für viele Mitarbeiter:innen in der Kriminalpolizei entfalten könnte. Viele Vorhaben und gute Ideen kosten nicht mal viel Geld und werden trotzdem nicht angegangen und umgesetzt.

Leistungsstarke Soft- und Hardware sind notwendig um erfolgreich ermitteln zu können. Hard- und Softwarebeschaffung ist zu bürokratisch und langwierig. Zu beschaffende Hardware/Technik ist bei erfolgter Lieferung teilweise schon wieder veraltet. Beschaffungswege

müssen beschleunigt und das Vergaberecht vereinfacht werden. Corona und unterbrochene Lieferketten haben die Beschaffungszeiten noch einmal deutlich verlängert.

Die Haushaltslage in M-V ist durch die Pandemie sehr angespannt, so dass Gelder für die Polizei nicht zur Verfügung stehen bzw. zur Verfügung gestellt werden. Neuanschaffung für Hard- und Software für die Kriminalpolizei werden genauestens geprüft und immer öfter in die Zukunft verschoben.

Punkt 5: Die Landesregierung wird aufgefordert, in Zusammenarbeit mit Sicherheitsbehörden, spezialisierten Verbänden und Vereinen sowie den Industrie- und Handelskammern die Sensibilität der Bürgerinnen und Bürger, Kommunen, Unternehmen und ihrer Beschäftigten weiter zu erhöhen sowie Beratungsangebote für Bürgerinnen und Bürger als auch Unternehmen zu ermöglichen oder zu unterstützen.

Eine Zusammenarbeit mit Kommunen, Unternehmen, Sicherheitsbehörden, Verbänden und Vereinen sowie den Industrie- und Handelskammern findet durch die ZAC M-V seit 2013 in Rahmen von Arbeitstreffen, Vorträgen (digital und analog) und Zeitschriftartikeln statt. Unternehmensverbände und/oder Vereine werden über aktuelle Phänomene, die Struktur der Landespolizei in Sachen Cybercrime-Bekämpfung und Präventionstipps informiert.

Dass dieses Beratungsangebot nicht ausreicht, liegt auf der Hand. Gegenwärtig wird diese Aufgabe durch zu wenig vorhandenes Personal beschränkt, so dass einzelne Unternehmen nicht proaktiv beraten werden können.

Bürgerinnen und Bürger werden im Rahmen von Anzeigenaufnahmen und Präventionsangeboten im Internet informiert.

Ein besonderes Augenmerk ist auf die KRITIS-Unternehmen zu richten, welchen eine herausragende Bedeutung im gesellschaftlichen Leben zugeschrieben wird und für die Stabilität der Gesellschaft wichtig sind.

KOST KRITIS (IM M-V)
Die KOST KRITIS im Innenministerium M-V soll zur Koordination von Aktivitäten zum KRITIS-Schutz und als Plattform zum Informationsaustausch dienen. Die Definition von KRITIS-Unternehmen richtet sich nach der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV).[17] Hierbei sind Schwellenwerte wie z.B.

- Anzahl von Einwohnern
- Anzahl von Patienten
- Anzahl von Passagieren
- Anzahl von Transaktionen
- Verpackungsmengen
- Mengenangaben in Litern, Gewicht

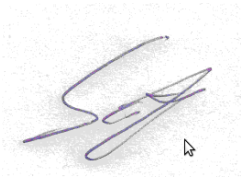
für die Einordnung von ausschlaggebender Bedeutung.

[17] https://www.gesetze-im-internet.de/bsi-kritisv/

Bis heute ist der Kriminalpolizei M-V nicht explizit von der KOST KRITIS gemeldet worden, welche Unternehmen in M-V diesen Kriterien entsprechen. Hierzu muss erwähnt werden, dass es KRITIS-Bund-Kriterien und daneben KRITIS-Land-Kriterien gibt. Die KRITIS-Land-Kriterien sind eher schwammig und stimmen nicht mit den strengen Schwellenwerten der BSI-KritisV überein.

Somit kann auch keine Beratung von KRITIS-Unternehmen, geschweige denn eine Vernetzung mit den richtigen Personen durch die Kriminalpolizei M-V stattfinden. Aufgrund der wirtschaftlichen Struktur in M-V dürften die hohen Schwellenwerte aus der BSI-KritisV für einen Großteil der Unternehmen aus M-V nicht zutreffen. Dennoch dürfte es vereinzelte Institutionen geben, die in das Raster fallen und Beratungsbedarf zu aktuellen Angriffsmethoden, Phänomenen und anderen relevanten Inhalten haben.

Mit freundlichen Grüßen



Stephan Gäfke
Vorsitzender des Bezirksverbandes Schwerin Bund Deutscher Kriminalbeamter M-V

Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V
Lennéstraße 1, Schloss · 19053 Schwerin

Landtag
Mecklenburg-Vorpommern
Ausschuss für Inneres, Bau
und Digitalisierung

- Der Vorsitzende -

AKTENZEICHEN
0.3.6.003/027/2022-01843

IHR ZEICHEN

IHRE NACHRICHT
vom 10. März 2022

AUSKUNFT

Telefon: 0385 59494-51
E-Mail: thomas.brueckmann@datenschutz-mv.de

22. März 2022

Antrag der Fraktion der FDP

Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen

Sehr geehrter Herr Mucha,

zunächst möchte ich mich für die Gelegenheit einer Stellungnahme und der Einladung zur Ausschuss-Sitzung bedanken.

Das Thema der Cyberkriminalität und deren Auswirkungen auf kritische Infrastrukturen haben, nicht zuletzt auch durch den russischen Angriff auf die Ukraine, eine erneut gestiegene Bedeutung erhalten. So erkennt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine abstrakt erhöhte Bedrohungslage für Deutschland an und ruft explizit Unternehmen, Organisationen und Behörden weiterhin dazu auf, ihre IT-Sicherheitsmaßnahmen zu erhöhen. In einer gemeinsamen Presseerklärung[1] mit dem Landeskriminalamt MV haben wir ebenfalls vor Cyber-Angriffswellen auf Einrichtungen und Unternehmen sowie vor gezielten Betrugsversuchen auf Bürgerinnen und Bürgern des Landes gewarnt.

Die Notwendigkeit einer Erhöhung der IT-Sicherheit und der Stärkung von vorhandenen Strukturen zu Bekämpfung von Cyberkriminalität, ergibt sich jedoch auch aus den jüngsten Vorfällen, die in Mecklenburg-Vorpommern zu beobachten waren.
So haben die erfolgreichen Angriffe auf den Landkreis Ludwigslust-Parchim und Schwerin, das Landesamt für innere Verwaltung MV sowie auf die Stadtwerke Wismar nachdrücklich gezeigt, dass Mecklenburg-Vorpommern im Visier von Cyberkriminellen steht und jederzeit mit erfolgreichen Angriffen gerechnet werden muss. Derartige Vorfälle schwächen bewusst auch das Vertrauen der Bevölkerung hinsichtlich der Leistungsfähigkeit des Staates, digitale Dienste sicher bereitzustellen und den Schutz der ihm anvertrauten personenbezogenen Daten zu gewährleisten.

Weiterhin konnte unsere Behörde im Zusammenhang mit der Meldepflicht von Verletzungen des Schutzes personenbezogener Daten (Datenpannenmeldung), die sich aus Artikel 33 der Datenschutzgrundverordnung (DS-GVO) ergibt, eine signifikante Steigerung von Vorfällen beobachten. So haben sich im Jahr 2021 die eingegangenen Meldungen von 259 Vorfällen, im

[1] https://www.datenschutz-mv.de/presse/?id=178879&processor=processor.sa.pressemitteilung

Vergleich zu 173 Vorfällen aus dem Vorjahr, um die Hälfte erhöht. Da eine derartige Datenpanne, die je nach Art und Umfang auch eine Benachrichtigung der Betroffenen vorsieht, mit einem enormen Reputationsverlust einhergeht, ist von einer deutlich höheren Dunkelziffer auszugehen.

Es ist dringend geboten die landesweit vorhanden Erkenntnisse aus Meldungen und Vorkommnissen zu bündeln. Hierbei ist unserer Ansicht nach insbesondere auch das Computer Emergency Response Team (CERT MV) in Ausstattung und in Befugnissen zu stärken, da sich dessen Reichweite bisher lediglich auf die Landesverwaltung erstreckt, nicht jedoch auf den kommunalen Bereich, obwohl dort sensibelste Daten von Bürgerinnen und Bürgern verarbeitet werden. Hier bietet sich auch eine verstärkte Zusammenarbeit mit unserer Behörde an, um Trends und Entwicklungen frühzeitig erkennen und bekämpfen zu können. Zudem müssen die Strukturen in den Landkreisen, Städten und Gemeinden hinreichend gestärkt werden, da nicht vorhandene oder offene IT-Stellen die Handlungsfähigkeit der hiesigen Verwaltung stark gefährden.

Dass eine funktionierende und sichere Informationstechnik einen zentralen Baustein für die Erreichung der Ziele der Landesverwaltung darstellt, zeigt auch das angedachte Gesetz zur Optimierung der IT-Landschaft in Mecklenburg-Vorpommern. Durch die Bündelung des vorhandenen IT-Personals, wird auch der Forderung der FDP Fraktion in Bezug auf mehr gut ausgebildetes Personal für den Bereich der IT-Sicherheit und Infrastruktur Rechnung getragen.

Sehr geehrter Herr Vorsitzender, wir unterstützen in Anbetracht der o.g. Ausführungen ausdrücklich den Antrag der Fraktion der FDP. Dem Landesbeauftragten für Datenschutz wurde jüngst eine Stelle für den Schwerpunkt Cyberkriminalität genehmigt. Unter den genannten Gesichtspunkten ist jedoch nur schwer vorstellbar, dass eine Stelle ausreichen wird, um dem gestiegenen Beratungs- und Kontrollbedarf im öffentlichen und nicht-öffentlichen Bereich und nicht zuletzt auch dem notwendigen Beratungsbedarf von Bürgerinnen und Bürgern des Landes gerecht zu werden. Insofern muss auch dem Landesbeauftragten für Datenschutz eine angemessene Ausstattung für die präventive Bekämpfung der Cyberkriminalität zur Verfügung gestellt werden.

Weiterhin geben wir zu Bedenken, dass auch das von uns immer wieder angesprochene Thema der digitalen Souveränität[2] eine entscheidende Rolle in Bezug auf die IT-Sicherheit spielt. Solange sich die Landesverwaltung weiterhin in eine kritische Technologieabhängigkeit von monopolartig organisierten Anbietern von Hard- und Software begibt, kann sie eine vollständige Kontrolle über die ihr anvertrauten Daten von Bürgerinnen und Bürgern nicht gewährleisten. Standardisierten Angriffen, wie wir sie beim Microsoft Exchange[3] Hack gesehen haben, kann nur begegnet werden, wenn die IT ausreichend diversifiziert ist und Open Source Technologien zum Einsatz kommen, die eine vollständige Kontrolle über die stattfindenden Datenverarbeitungen ermöglicht.

Mit freundlichen Grüßen
im Auftrag

Thomas Brückmann

[2] https://www.datenschutz-mv.de/presse/?id=168438&processor=processor.sa.pressemitteilung
[3] https://www.datenschutz-mv.de/presse/?id=168262&processor=processor.sa.pressemitteilung