Landtag von Baden-Württemberg **Drucksache 16 / 5779**

16. Wahlperiode **20. 02. 2019**

Antrag

der Abg. Daniel Karrais u. a. FDP/DVP

und

Stellungnahme

des Ministeriums für Inneres, Digitalisierung und Migration

IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und generelle Zahl der IT-Sicherheitsvorfälle

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche neuen Erkenntnisse sie bezüglich Hacker-Angriffen auf KRITIS im Zeitraum vom 1. Januar 2018 bis 31. Dezember 2018 erlangt hat;

2. inwiefern sich die Zahl der Hacker-Angriffe auf das Stromnetz in Baden-Württemberg im Zeitraum vom 1. Januar 2013 bis zum 31. Dezember 2018 entwickelt hat;

3. welche Maßnahmen sie seit Februar 2018 getroffen hat, um Cyber-Angriffe auf das Stromnetz abzuwehren und im Vorhinein zu verhindern;

4. wie sie zusammen mit Netzbetreibern und Stadtwerken kooperiert, um eine Verbesserung der IT-Sicherheit der Energieversorgung zu erwirken;

5. wie sie die Schaffung einer Rechtsgrundlage für Analyse und bedarfsgerechte Speicherung von Protokolldaten bewertet, wie das die Bundesländer Niedersachsen, Sachsen und das Saarland derzeit tun;

6. wie sie zur Schaffung einer zentralen Behörde − wie in Bayern das Landesamt für Sicherheit in der Informationstechnik (LSI) − steht und ob sie ähnliche Pläne für Baden-Württemberg hat;

7. inwieweit sie Kenntnis davon hat, wie sich die Qualität der Angriffe auf KRITIS verändert hat (Sabotage statt Spionage);

8. welche Erkenntnisse sie zu den strategischen Zielen der die Sabotage versuchenden Hacker hat;

Eingegangen: 20. 02. 2019 / Ausgegeben: 21. 03. 2019

9. welche Erkenntnisse sie hat, aus welchen Staaten die Hackerangriffe kommen;

10. welche Erkenntnisse sie hat, für welche ausländischen Organisationen die Hacker arbeiten;

11. inwieweit Hacker ihre Angriffe über Infrastrukturbestandteile ausübten, die aus Ländern geliefert wurden, aus denen auch die Hacker kommen;

12. welche außerordentlichen Maßnahmen sie treffen will, um die anstehenden Wahlen in den Kommunen und Europa zu schützen;

13. inwiefern sich die Zahl der Hacker-Angriffe auf baden-württembergische kleine und mittelständische Unternehmen im Zeitraum vom 1. Januar 2013 bis zum 31. Dezember 2018 entwickelt hat;

14. welche Maßnahmen in den Landesbehörden getroffen werden, um Standardmaßnahmen zur IT-Sicherheit zu fördern (HTTPS-Protokoll auf behördlichen Websites).

20. 02. 2019

Karrais, Weinmann, Dr. Rülke, Brauer,
Keck, Dr. Schweickert, Dr. Goll FDP/DVP

Begründung

Die Welt am Sonntag berichtete am 17. Februar 2019 unter Berufung auf bislang nichtveröffentlichte Zahlen des Bundesamts für Sicherheit in der Informationstechnik (BSI) von einem Anstieg der Hacker-Angriffe gegen KRITIS − vor allem gegen das Stromnetz. Der Behördenspiegel vom Februar 2019 („Den Datenverkehr im Blick“) berichtet von Gesetzesinitiativen anderer Bundesländer in Bezug auf Rechtsgrundlagen zur Überwachung von IT-Systemen.

Der Antrag soll zudem die Erkenntnisse aus der Große Anfrage der FDP/DVP-Fraktion (Drucksache 16/3345) aktualisiert ergänzen.

Stellungnahme

Mit Schreiben vom 14. März 2019 Nr. 6-45/7 nimmt das Ministerium für Inneres, Digitalisierung und Migration im Einvernehmen mit dem Staatsministerium, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau, dem Ministerium für Soziales und Integration, dem Ministerium für Ländlichen Raum und Verbraucherschutz, dem Ministerium der Justiz und für Europa und dem Ministerium für Verkehr zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche neuen Erkenntnisse sie bezüglich Hacker-Angriffen auf KRITIS im Zeitraum vom 1. Januar 2018 bis 31. Dezember 2018 erlangt hat;

Zu 1.:

Zum Rechtsrahmen für die IT-Sicherheit Kritischer Infrastrukturen und damit insbesondere auch die Vorgaben für Meldepflichten von Sicherheitsvorfällen wird auf die Antwort zu den Fragen Nr. 1 und 2 der vorangegangenen Großen Anfrage „IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und Institutionen im beson-

deren staatlichen Interesse (INSI)“ der FDP/DVP-Fraktion (Drucksache 16/3345) verwiesen.

Im Zeitraum vom 1. Januar 2018 bis 31. Dezember 2018 wurden drei Cyberangriffe im Zusammenhang mit KRITIS-Unternehmen im Land bekannt, die allesamt einen mutmaßlich nachrichtendienstlichen Hintergrund hatten.

2. inwiefern sich die Zahl der Hacker-Angriffe auf das Stromnetz in Baden-Württemberg im Zeitraum vom 1. Januar 2013 bis zum 31. Dezember 2018 entwickelt hat;

Zu 2.:

Über Angriffe aus den Jahren 2013 bis 2016 liegen keine Erkenntnisse vor.

Nach Mitteilung des Landesamtes für Verfassungsschutz (LfV) wurden in den Jahren 2017 und 2018 insgesamt fünf Fallkomplexe im Zusammenhang mit Cyberangriffen gegen IT-Infrastrukturen/-netze von Stromnetzbetreibern in Baden-Württemberg bearbeitet.

3. welche Maßnahmen sie seit Februar 2018 getroffen hat, um Cyber-Angriffe auf das Stromnetz abzuwehren und im Vorhinein zu verhindern;

Zu 3.:

Wie in der Antwort zu Frage 4 der vorangegangenen Großen Anfrage (Drucksache 16/3345) dargestellt, sind Stromnetzbetreiber zur Umsetzung von IT-sicherheitstechnischen Mindeststandards verpflichtet. Durch das Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) hat die Bundesnetzagentur den Auftrag erhalten, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog entsprechender Sicherheitsanforderungen zu erstellen.

Gleichzeitig unterstützt das LfV die Unternehmen im Land – insbesondere auch KRITIS-Unternehmen wie beispielsweise Stromnetzbetreiber – bei der Detektion, Attribution und Prävention von bzw. vor Cyberspionage- und Cybersabotageangriffen mit (mutmaßlich) nachrichtendienstlichem Hintergrund.

Die Themenfelder Cyberspionage und Cybersabotage nehmen bei der präventiven Arbeit des LfV einen breiten Raum ein. Im Rahmen von zahlreichen anlassunabhängigen Beratungen und Sensibilisierungsveranstaltungen sowie über einen wöchentlichen Newsletter werden Unternehmen an die Thematik herangeführt und über Schutzmöglichkeiten informiert. Darüber hinaus ist das LfV im Sicherheitsforum Baden-Württemberg („Sicherheitsforum Baden-Württemberg – Die Wirtschaft schützt ihr Wissen“) aktiv und leistet auch in diesem Zusammenhang Präventionsarbeit.

Teil der präventiven Aufgabenbewältigung des LfV ist es ferner, potenziell betroffene Unternehmen im Vorfeld zu warnen und zu sensibilisieren. Bei konkreten Verdachtsfällen finden anlassbezogene Sensibilisierungsgespräche mit den mutmaßlich konkret betroffenen Unternehmen statt. Hierbei werden nach Möglichkeit technische Indikatoren des jeweiligen Angriffs übermittelt, tiefergehende Analysemöglichkeiten und Analyseparameter aufgezeigt, Angriffsvektoren beschrieben und adäquate Schutzmaßnahmen vorgeschlagen.

Das LfV hat darüber hinaus keine Befugnisse, Cyberangriffe aktiv abzuwehren. Das LfV unterstützt jedoch betroffene Unternehmen bei der Aufarbeitung von Angriffen mit mutmaßlich nachrichtendienstlichem Hintergrund.

Die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts (LKA) unterhält auch anlassunabhängig zu Unternehmen der Kritischen Infrastruktur, wie beispielsweise den Stromnetzbetreibern, einen engen Kontakt und tauscht sich regelmäßig zum Thema Cybersicherheit aus. Zudem werden vorliegende Erkenntnisse über aktuelle Bedrohungslagen durch die ZAC in Form von Warn- und Informationsmeldungen an die relevanten Unternehmen gesteuert.

Als polizeilicher „Single Point of Contact“ gewährleistet die ZAC eine durchgehende telefonische und elektronische Erreichbarkeit, um IT-Sicherheitsvorfälle entgegenzunehmen und zeitnah polizeiliche Erstmaßnahmen zu veranlassen.

Im Rahmen des CyberSicherheitsForums im Februar 2019, einer gemeinsamen Veranstaltung des Ministeriums für Inneres, Digitalisierung und Migration und des LKA, war eine eigene Vortragsreihe dem Themenfeld „Cybersicherheit für Kritische Infrastrukturen“ gewidmet.

4. wie sie zusammen mit Netzbetreibern und Stadtwerken kooperiert, um eine Verbesserung der IT-Sicherheit der Energieversorgung zu erwirken;

Zu 4.:

Wie in der Antwort zu Frage 3 dargestellt, stehen LfV und LKA bei Fragen zur Verbesserung der IT-Sicherheit grundsätzlich allen Netzbetreibern und Stadtwerken im Land als Ansprechpartner zur Verfügung.

Das LfV pflegt etablierte Kontakte mit einzelnen Netzbetreibern und Unternehmen aus dieser Branche und sucht darüber hinaus auch intensiven Kontakt zu diversen „Multiplikatoren“ wie Verbänden, Arbeitsgemeinschaften und Arbeitskreisen der Energiewirtschaft, um diese im Sinne einer „Hilfe zur Selbsthilfe“ zu informieren und zu sensibilisieren. Die ergriffenen Maßnahmen zielen darauf ab, bei den relevanten Unternehmen eine generelle Verbesserung der IT-Sicherheit zu erwirken, das Bewusstsein für Cyberangriffe mit nachrichtendienstlichem Hintergrund zu erhöhen und potenzielle Betroffenheit frühzeitig entdecken zu können.

Ebenso führt das LKA in enger Zusammenarbeit mit Organisationen wie dem Verband kommunaler Unternehmen (VkU) regelmäßig Awarenessveranstaltungen durch.

Darüber hinaus ist eine gemeinsame Cyberübung des LKA mit dem VkU sehr zeitnah terminiert. Weitere derartige Übungen mit KRITIS-Unternehmen sind bereits in Planung.

5. wie sie die Schaffung einer Rechtsgrundlage für Analyse und bedarfsgerechte Speicherung von Protokolldaten bewertet, wie das die Bundesländer Niedersachsen, Sachsen und das Saarland derzeit tun;

Zu 5.:

Die Landesverwaltung beabsichtigt, ihre derzeit getroffenen Maßnahmen zur Auswertung von Systemprotokollen im Zuge der Fortführung der IT-Neuordnung und der damit verbundenen weiteren Standardisierung ihrer IT-Systeme auszubauen.

In einem ersten Schritt sollen dazu Lösungen zur automatisierten Protokollauswertung, zum Erkennen von Angriffen und zum automatischen Einleiten von Abwehrmaßnahmen in Einsatz gebracht werden. Unmittelbar hierfür werden zunächst keine weiterführenden gesetzlichen Grundlagen benötigt.

6. wie sie zur Schaffung einer zentralen Behörde − wie in Bayern das Landesamt für Sicherheit in der Informationstechnik (LSI) − steht und ob sie ähnliche Pläne für Baden-Württemberg hat;

Zu 6.:

Das Ministerium für Inneres, Digitalisierung und Migration erarbeitet aktuell Vorschläge für eine Verbesserung der bestehenden Cybersicherheitsarchitektur sowie eine Cybersicherheitsstrategie für Baden-Württemberg. Dabei werden auch Erfahrungen aus anderen Ländern ausgewertet, einschließlich des in Bayern eingerichteten Landesamts für Sicherheit in der Informationstechnik (LSI). Konkrete Ergebnisse dazu liegen noch nicht vor.

7. inwieweit sie Kenntnis davon hat, wie sich die Qualität der Angriffe auf KRITIS verändert hat (Sabotage statt Spionage);

Zu 7.:

Grundsätzlich eignet sich jeder Cyberspionageangriff technisch und methodisch dazu, auch Cybersabotageangriffe vorzubereiten oder durchzuführen. Hat sich ein Angreifer einmal unbefugten Zugang zu einem IT-System verschafft, besteht dort einerseits die Möglichkeit, Daten zu entwenden, und andererseits die Möglichkeit, Daten zu löschen oder zu manipulieren.

Es erscheint naheliegend, dass bei Cyberangriffen gegen KRITIS-Unternehmen zunächst das Ziel verfolgt wird, möglichst langfristig und unentdeckt sensible Informationen auszuspähen, um weiter in das „Opfersystem“ vordringen zu können und so gegebenenfalls auch Cybersabotageangriffe vorbereiten zu können.

Ein erfolgreiches Eindringen beispielsweise in die direkte Anlagensteuerung eines Kraftwerks durch einen netzwerkgestützten Angriff von außen konnte bislang noch nicht nachgewiesen werden. Dennoch beobachtet das LfV die Entwicklung der steigenden – informationstechnischen wie methodischen – Qualität der Angriffe auf KRITIS-Unternehmen mit Sorge.

8. welche Erkenntnisse sie zu den strategischen Zielen der die Sabotage versuchenden Hacker hat;

Zu 8.:

Die Täterstrukturen setzen sich nach polizeilicher Erfahrung vielfältig zusammen und reichen von Angreifern mit durchschnittlichen IT-Kenntnissen und autodidaktisch erworbenen Fähigkeiten zu Cyberangriffen bis hin zu fachlich versierten Tätern. Die zugrunde liegenden Motive können von Profitstreben über Sabotage- bis hin zu Spionageabsichten reichen.

Die Motivation fremder Staaten beziehungsweise ihrer Nachrichtendienste könnte darin bestehen, sich auf mögliche Konfliktlagen mit den angegriffenen Staaten vorzubereiten und sich so im Falle von politischen, wirtschaftlichen oder im Vorfeld möglicher militärischer Auseinandersetzungen strategische, taktische und/-oder technische Vorteile zu verschaffen. Ein eventuell lang andauernder Ausfall eines oder gar mehrerer KRITIS-Unternehmen beziehungsweise der entsprechenden Infrastrukturen könnte weitreichende negative Folgen für das betroffene Gemeinwesen nach sich ziehen. Das Schadpotenzial derartiger Attacken ist dementsprechend sehr hoch.

9. welche Erkenntnisse sie hat, aus welchen Staaten die Hackerangriffe kommen;

10. welche Erkenntnisse sie hat, für welche ausländischen Organisationen die Hacker arbeiten;

Zu 9. und 10.:

Hauptakteure im Bereich mutmaßlich nachrichtendienstlich gesteuerter Cyberangriffe fremder Staaten, die sich in den letzten Jahren gegen baden-württembergische Einrichtungen und Unternehmen richteten, sind Russland, Iran und China. Bei diesen Cyberattacken arbeiten die Angreifer letztlich für fremde Nachrichtendienste, denen sie entweder unmittelbar selbst angehören oder durch welche sie mittelbar mit der Angriffsdurchführung beauftragt wurden.

11. inwieweit Hacker ihre Angriffe über Infrastrukturbestandteile ausübten, die aus Ländern geliefert wurden, aus denen auch die Hacker kommen;

Zu 11.:

Dem LfV liegen weder technische Belege noch konkrete Hinweise Dritter, wie etwa vonseiten des BSI, dazu vor, dass Angriffe über Infrastrukturbestandteile ausgeübt werden, die aus den Ländern der Angreifer geliefert wurden.

12. welche außerordentlichen Maßnahmen sie treffen will, um die anstehenden Wahlen in den Kommunen und Europa zu schützen;

Zu 12.:

Abstrakten Gefahren, die von möglichen Cyberangriffen auf Wahlen ausgehen, kommt eine hohe Bedeutung zu. Eine Manipulation der vorläufigen Wahlergebnisse – oder eine Störung bei der Ermittlung dieser Ergebnisse – würde das Ansehen der Wahlorgane und das Vertrauen in die demokratischen Prozesse beeinträchtigen. Entsprechend hoch ist die Sensibilität hinsichtlich relevanter Sicherheitsaspekte bei allen Beteiligten – Bund, Ländern und Kommunen, IT-Sicherheitsbehörden, aber auch den Softwareherstellern.

Im Vorfeld der Europawahl am 26. Mai 2019 wurden bislang deshalb unter anderem folgende Schutzmaßnahmen getroffen:

Im Auftrag der EU-Kommission wurde unter Beteiligung des BSI ein Kompendium erarbeitet, das eine Sammlung von relevanten Themen, Risiken und Maßnahmen im Bereich Cybersicherheit bereitstellt.

Sowohl auf europäischer als auch auf nationaler Ebene wurden Netzwerke eingerichtet, um durch einen schnellen Informationsaustausch potenzielle Bedrohungen für die Europawahlen rasch identifizieren und ihnen entgegenwirken zu können. Baden-Württemberg ist in diese Netzwerke eingebunden.

Das BSI hat im Jahr 2018 in enger Zusammenarbeit mit dem Bundeswahlleiter und den Landeswahlleitungen Vorschläge zur Absicherung der Übermittlung der vorläufigen Ergebnisse bei der kommenden Europawahl ausgearbeitet. Diese beinhalten technische und organisatorische Schritte rund um den Einsatz von Informationstechnik, um so die Integrität und Verfügbarkeit der Wahlergebnisse sicherzustellen. Die Landeswahlleiterin, die für die Vorbereitung und Durchführung der Europawahl in Baden-Württemberg zuständig ist, hat diese technischen und organisatorischen Aspekte an die Wahlleitungen der Stadt- und Landkreise und über diese allen Kommunen weitergeleitet, damit diese die Gegebenheiten vor Ort prüfen und rechtzeitig vor der Wahl dafür Sorge tragen, dass gegebenenfalls noch bestehende Sicherheitslücken beseitigt werden.

Darüber hinaus wird es auf allen Ebenen noch eine Reihe von weiteren organisatorischen und technischen Vorkehrungen geben, um die Ermittlung des vorläufigen Wahlergebnisses in der Wahlnacht zu sichern. Aus Sicherheitsgründen können auch diese jedoch nicht offengelegt werden.

Das endgültige Wahlergebnis wird bei allen Wahlen auf der Grundlage der schriftlichen Wahlniederschriften der einzelnen Wahlorgane ermittelt und daher durch Cyberangriffe grundsätzlich nicht tangiert.

Die Kommunalwahlen werden von den Kommunen als Selbstverwaltungsaufgabe eigenverantwortlich im Rahmen des geltenden Rechts durchgeführt. Dies umfasst auch die Entscheidung, ob und gegebenenfalls welche IT-Verfahren bei der Vorbereitung und Durchführung der Kommunalwahlen eingesetzt werden.

Zur Ergebniszusammenstellung und -übermittlung der Wahlergebnisse kommen bei den Kommunalwahlen in der Regel dieselben Fachanwendungen wie bei der Europawahl zum Einsatz. Werden die für die Europawahl aufgestellten Anforderungen an die IT-Sicherheit und die sonstigen Organisationsaspekte berücksichtigt, dürfte die korrekte und sichere Ermittlung der Ergebnisse der Kommunalwahlen gleichfalls gewährleistet sein.

13. inwiefern sich die Zahl der Hacker-Angriffe auf baden-württembergische kleine und mittelständische Unternehmen im Zeitraum vom 1. Januar 2013 bis zum 31. Dezember 2018 entwickelt hat;

Zu 13.:

Hinter den als sogenannte „Hacker-Angriffe“ bezeichneten Handlungen stehen im strafrechtlichen Sinne häufig Delikte des Ausspähens und Abfangens von Daten gemäß §§ 202 a, 202 b StGB sowie Delikte der Datenveränderung und Computersabotage gemäß §§ 303 a, 303 b StGB.

Die Fallzahlen in diesen Bereichen machen in Relation zu den Gesamtfallzahlen der Internet- und Computerkriminalität lediglich einen geringen prozentualen Anteil aus. Allerdings ist erfahrungsgemäß von einem sehr hohen Dunkelfeld auszugehen. Sicherheitsvorfälle im IT-Umfeld werden von geschädigten Unternehmen, beispielsweise aus Angst vor einem Reputationsverlust, häufig nicht angezeigt.

Die ZAC des LKA verzeichnet in ihrer internen Statistik eine ansteigende Tendenz hinsichtlich Cyberangriffen auf Unternehmen:

Während im Jahr 2015 bei insgesamt 488 Kontaktaufnahmen mit der ZAC 183 Straftaten zum Nachteil von Wirtschaftsunternehmen zur Anzeige gebracht wurden, waren es im Jahr 2018 bei insgesamt 805 Kontaktaufnahmen bereits 453 angezeigte Straftaten.

Neben Einflüssen durch ein möglicherweise geändertes Anzeigeverhalten dürfte diese Entwicklung insbesondere auf die zunehmende Digitalisierung kleiner und mittelständischer Unternehmen (KMU) zurückzuführen sein.

Nach Erkenntnissen des LfV sind im Übrigen vermehrt Dienstleister und Kunden von KRITIS-Betreibern in den Fokus fremder Nachrichtendienste geraten. Das LfV geht ebenfalls von einem nicht genau quantifizierbaren hohen Dunkelfeld in diesem Bereich aus.

Gerade für KMU ist IT-Sicherheit ein essenzielles Thema. Daher unterstützt das Land insbesondere auch KMU auf der präventiven Seite, beispielsweise über das Karlsruher Forschungszentrum Informatik (FZI) und das Digitale Innovationszentrum (DIZ) sowie durch wirtschaftsnahe Forschung.

14. welche Maßnahmen in den Landesbehörden getroffen werden, um Standardmaßnahmen zur IT-Sicherheit zu fördern (HTTPS-Protokoll auf behördlichen Websites).

Zu 14.:

Die Verwendung des Hypertext Transfer Protocol Secure (HTTPS) als sicheres Übertragungs- bzw. Kommunikationsprotokoll für Websites und Webportale ist in der 2018 neu verabschiedeten Verwaltungsvorschrift des Ministeriums für Inneres, Digitalisierung und Migration über IT-Standards des Landes (VwV IT-Standards) manifestiert. Viele bestehende, für den Auf- und Ausbau des E-Governments grundlegende und wichtige Portale, beispielsweise *https://service-bw.de*, sind bereits ausschließlich verschlüsselt aufrufbar.

In den Landesbehörden befinden sich im Zuge der Umsetzung der Verwaltungsvorschrift des Ministeriums für Inneres, Digitalisierung und Migration zur Informationssicherheit (VwV Informationssicherheit) vielfältige technische und strategische Maßnahmen in Umsetzung oder – sofern entsprechende Ressourcen hierfür generiert werden müssen – in Planung. Solche Maßnahmen sind beispielsweise die Durchführung von Schwachstellenscans und Penetrationstests für Web-Anwendungen und die entsprechende Optimierung der untersuchten Anwendungen.

Besondere Bedeutung kommt dabei der nach der Methodik des BSI IT-Grundschutz geforderten Erstellung von Sicherheitskonzepten für alle eingesetzten IT-Anwendungen zu. Hierbei gilt es, die im Verantwortungsbereich der Einrichtungen und Dienststellen der Landesverwaltung stehenden zahlreichen Verfahren nach ei-

ner standardisierten Vorgehensweise zu untersuchen, Maßnahmen nach Vorgaben des BSI umzusetzen und die Umsetzungsstände zu dokumentieren. Dieser Prozess muss aufgrund sich ändernder Rahmenbedingungen regelmäßig neu durchlaufen werden.

Bei der technischen Umsetzung der Sicherheitskonzepte liegt ein Schwerpunkt auf dem weiteren Ausbau des Einsatzes von Verschlüsselungsmethoden – sowohl auf Transportebene (Landesverwaltungsnetz) als auch auf Anwendungs- und Verbindungsebene, bei Webauftritten durch die Nutzung des HTTPS.

Um insbesondere den sich rasch verändernden technischen Gegebenheiten angemessen Rechnung zu tragen, ist die Erstellung und Revision der Sicherheitskonzepte für IT-Anwendungen eine Daueraufgabe. Hierdurch entstehen beständig Aufwände in den Behörden und bei den eingesetzten IT-Dienstleistern, welche künftig zusätzliche Ressourcen erfordern werden.

In Vertretung

Klenk

Staatssekretär