Landtag von Baden-Württemberg **Drucksache 17 / 483**

17. Wahlperiode **9.7.2021**

Antrag

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

und

Stellungnahme

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Cyberangriffe und Maßnahmen zur Stärkung der IT-Sicherheit

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie viele Cyberangriffe auf die IT-Infrastruktur bei Behörden und sonstigen Einrichtungen des Landes und der Kommunen sowie Unternehmen in Baden-Württemberg im Jahr 2020 sowie in der ersten Jahreshälfte 2021 jeweils erfolgt sind;

2. um welche Art von Angriffen es sich jeweils handelte und welche Folgen daraus für die Betroffenen jeweils resultierten (wie z. B. Datendiebstahl, Erpressungsversuche, unwiederbringliche Löschung von Daten);

3. wie viele Meldungen welcher Art in der ersten Jahreshälfte 2021 bei der Cybersicherheitsagentur (CSBW) eingegangen und gebündelt worden sind;

4. wie viele private Unternehmen und Behörden in Baden-Württemberg oder Behörden, Organisationen oder sonstige Einrichtungen des Landes Baden-Württemberg vom aktuellen Hackerangriff der Gruppe „REvil“ auf den IT-Dienstleister Kaseya in welchem Ausmaß jeweils mit welchen Auswirkungen betroffen sind;

5. welchen Handlungsbedarf und welche Möglichkeiten sie für das Land bei der Prävention im Bereich der Cybersicherheit für private Unternehmen sieht, insbesondere auch im Hinblick darauf, warum die Cybersicherheitsagentur keine ausführlichen Beratungsleistungen in diesem Sinn übernehmen soll (wie die Stellungnahme zu Ziffer 13 in Drucksache 16/9306 nahelegt);

Eingegangen: 9.7.2021 / Ausgegeben: 16.8.2021

6. welche Maßnahmen sie trifft, um Cyberangriffe auf die Durchführung der Bundestagswahlen 2021 in Baden-Württemberg zu verhindern und dadurch einen ordnungsgemäßen Verlauf von Durchführung, Auszählung und Ergebnisübertragung garantieren kann;

7. welche Kenntnisse sie, insbesondere über das Landesamt für Verfassungsschutz oder die Cybersicherheitsagentur, über drohende oder durchgeführte Cyberangriffe und Manipulationen zur Einflussnahme im Zusammenhang mit der Bundestagswahl 2021 und dem dazugehörigen Wahlkampf hat;

8. welche Vorbereitungen und Maßnahmen sie trifft, um Angriffe und Manipulation zur Einflussnahme über soziale Medien und IT-Infrastrukturen von Bewerberinnen und Bewerbern zur Bundestagswahl 2021 sowie betroffene Parteien zu verhindern;

9. wie sich die Zahl der Anfragen bei der Cyberwehr seit dem Beginn der zweiten Projektphase am 1. September 2020, aufgeschlüsselt nach Monaten, entwickelt hat (auch im Vergleich zur Zeit der Pilotprojektphase);

10. zu welchen Themen diese erfolgten;

11. bis wann sie eine finanzielle Förderung der Cyberwehr durch das Land in welchem Umfang fortführen wird bzw. plant fortzuführen;

12. inwieweit sich die Tätigkeitsbereiche von Cyberwehr und CSBW überschneiden und insoweit zukünftig ausgestaltet werden sollen.

9.7.2021

Karrais, Goll, Haußmann, Dr. Timm Kern, Birnstock, Bonath, Brauer, Fischer, Haag, Heitlinger, Dr. Jung, Reith, Scheerer, Dr. Schweickert, Trauschel FDP/DVP

Begründung

Die Zahl der Cyberangriffe auf Unternehmen und Behörden nimmt stetig zu, die Folgen können dabei immens sein. Der jüngst bekannt gewordene Angriff der Hackergruppierung „REvil“, der Unternehmen weltweit betrifft, macht dies exemplarisch deutlich. Gerade auch im Hinblick auf die Durchführung der Bundestagswahl 2021 sind Cyberangriffe und versuchte Einflussnahme zu befürchten, die es zu verhindern gilt. Prävention und Sensibilisierung im Bereich der IT-Sicherheit, die das Bewusstsein für die Notwendigkeit einer Absicherung von IT-Systemen und sensiblen Daten stärkt, ist daher unabdingbar. Deshalb braucht es aus Sicht der Antragsteller effektive Hilfestellungen für Unternehmen und klare Zuständigkeiten zwischen den staatlichen Stellen im Bereich der Cybersicherheit, insbesondere auch im Hinblick auf die Ausgestaltung der Cybersicherheitsagentur und der Cyberwehr.

Stellungnahme

Mit Schreiben vom 3. August 2021 Nr. IM7-0141.5-135/20/9 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Kultus, Jugend und Sport, dem Ministerium für Wissenschaft, Forschung und Kunst und dem Ministerium für Wirtschaft, Arbeit und Tourismus zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. *wie viele Cyberangriffe auf die IT-Infrastruktur bei Behörden und sonstigen Einrichtungen des Landes und der Kommunen sowie Unternehmen in Baden-Württemberg im Jahr 2020 sowie in der ersten Jahreshälfte 2021 jeweils erfolgt sind;*

2. *um welche Art von Angriffen es sich jeweils handelte und welche Folgen daraus für die Betroffenen jeweils resultierten (wie z. B. Datendiebstahl, Erpressungsversuche, unwiederbringliche Löschung von Daten);*

3. *wie viele Meldungen welcher Art in der ersten Jahreshälfte 2021 bei der Cybersicherheitsagentur (CSBW) eingegangen und gebündelt worden sind;*

Zu 1. bis 3.:

Hinsichtlich der Verwendung der Begriffe „Cyberangriffe“ und „Angriffe“ wird auf die Antworten zu den Ziffern 1, 2 und 5 des Antrags „IT-Sicherheitsvorfälle in Baden-Württemberg“ der FDP/DVP-Fraktion (Drucksache 16/8662) verwiesen, ebenso auf die Antwort zu Ziffer 1 des Antrags „Cyberangriffe auf Landesbehörden“ der SPD-Fraktion (Drucksache 16/7020).

Dabei ist nochmals herauszustellen, dass solche Angriffe täglich und rund um die Uhr sowohl auf Institutionen der Landesverwaltung als auch der mittelbaren Staatsverwaltung massenhaft stattfinden. Bei der Beantwortung der Fragen dieses Antrages wird daher unterstellt, dass mit „Angriffen“ im Sinne der Fragen des vorliegenden Antrags erfolgreiche Angriffe gemeint sind, also solche, die als „Sicherheitsvorfall“ einzustufen und zu behandeln waren.

Insgesamt waren im angefragten Zeitraum zehn Angriffe auf die IT-Infrastruktur bei Behörden und sonstigen Einrichtungen des Landes zu verzeichnen, die einen Einfluss auf die betroffenen Systeme und deren Funktion und Verfügbarkeit hatten. In zwei Fällen erfolgte ein sogenannter „Distributed Denial of Service“ (DDoS) Angriff auf zentrale Web-Plattformen. Ein solcher Angriff zielt auf die Überlastung von Webservern und Online-Services. Allerdings sind solche Angriffe durch ad-hoc-Maßnahmen an den zentralen Firewalls sehr schnell eindämmbar. Daher führten die Angriffe meist nur zu sehr kurzfristigen Störungen. Bei einem der benannten DDoS-Angriffe handelte es sich um eine Serie von über mehrere Tage verteilt erfolgten, gleichgelagerten Angriffen auf die Moodle-Lernplattformen. Diese waren zu Beginn des Online-Unterrichts in der Anfangszeit der Pandemiebewältigungsphase besonders im Fokus von Angriffen. Nachdem der erste Angriff auf die Moodle-Plattform zu einem halbtägigen Ausfall einzelner Server führte, konnten die weiteren Angriffe in den ersten Minuten erfolgreich abgewehrt werden. Bei zwei anderen Vorfällen wurden Systeme so manipuliert, dass deren Rechenleistung kurzfristig zum Erzeugen von Kryptowährungen (sogenanntes „Krypto-Mining“) missbraucht wurde. Dies führte zu partiellen Ausfällen der auf diesen Systemen laufenden Dienste. Nachdem die Schadsoftware entfernt, die ausgenutzten Schwachstellen beseitigt und weitere Sicherheitsmaßnahmen umgesetzt worden waren, konnten die Systeme wieder in Betrieb genommen werden. Wiederum in zwei weiteren Fällen wurden Daten in geringem Umfang teilweise verschlüsselt und gelöscht. Diese konnten aus Backups wiederhergestellt werden.

Die Systeme wurden dazu neu aufgesetzt und vor Inbetriebnahme einer erweiterten Sicherheitsprüfung unterzogen. Bei einem Angriff auf eine einfache, wenig frequentierte Webseite gelang es den Angreifern, Inhalte zu manipulieren und die Seitenaufrufe für kurze Zeit auf eine pornografische Seite umzuleiten. Der Angriff wurde nach kürzester Zeit erkannt, die Manipulation rückgängig gemacht und weitere Angriffe abgewehrt. Bei einem anderen Webservice wurden eingebundene Kontaktformulare unerlaubt dazu genutzt, erpresserische E-Mails an Mitarbeitende der Landesverwaltung zu senden. Durch Sensibilisierungsmaßnahmen und automatisierte Filterung ist kein Schaden entstanden. Die ausgenutzte Lücke wurde umgehend geschlossen. In zwei anderen Fällen wurden Angriffe noch in ihrem jeweiligen Verlauf erkannt, Gegenmaßnahmen rechtzeitig eingeleitet und somit der Erfolg der Angriffe vereitelt. Im Zuge der Maßnahmen mussten die Systeme und Services für kurze Zeit teilweise außer Betrieb genommen werden. Da im Mittelpunkt der Angriffe immer wieder Webservices stehen, wurden gezielte Maßnahmen zur verstärkten Absicherung und Überwachung umgesetzt.

Im kommunalen Bereich war im Jahr 2020 und in der ersten Jahreshälfte 2021 nach Meldung des zentralen IT-Dienstleisters der Kommunen Komm.ONE jeweils eine einstellige Anzahl an Sicherheitsvorfällen zu verzeichnen. Die dort erfolgten Angriffe sind in ihrer Art vielschichtig. So kommen allgemeine Angriffe über E-Mail oder Social Engineering vor. Aber auch gezielte Angriffe auf einzelne Institutionen und Personen sind erkennbar. Das Ziel ist häufig eine Monetarisierung, entweder durch Erpressung oder durch das Erschleichen von Zahlungen. Auch die Nutzung von vertrauenswürdigen Seiten für unlautere Handlungen ist zu beobachten. Soweit es der Komm.ONE bekannt ist, wurden die Angriffe allesamt rechtzeitig bemerkt und es sind keine nennenswerten Schäden eingetreten. Zur Wahrung der Vertraulichkeit sind keine näheren Angaben möglich.

Für den Zeitraum vom 1. Januar 2020 bis 30. Juni 2021 liegen dem Landesamt für Verfassungsschutz Baden-Württemberg (LfV) Hinweise zu Cyberangriffen mit mutmaßlich nachrichtendienstlichem Hintergrund im höheren zweistelligen Bereich vor. Im Fokus standen Einrichtungen des Landes, Kommunen und Unternehmen in Baden-Württemberg.

Cyberakteure mit staatlichem Hintergrund haben ein großes Interesse daran, möglichst lange und unerkannt Informationen zu gewinnen. Zwar ist bei staatlichen Akteuren nicht auszuschließen, dass sie Sabotageaktionen (z. B. das Löschen oder Verschlüsseln von Daten) in oder an kompromittierten IT-Systemen vorbereiten. Belastbare Erkenntnisse darüber oder über daraus resultierende Erpressungsversuche liegen dem LfV indes nicht vor.

Staatliche Akteure nutzen u. a. folgende Methoden zum Erreichen ihrer Ziele:

- Angriffe gegen IT-Infrastruktur
- E-Mail-Versand mit beigefügter Malware
- E-Mail-Versand mit enthaltenen Links zu Webseiten mit Schadfunktion
- (Spear)-Phishing-Angriffe zum Abgreifen von Zugangsdaten
- Angriffe auf mit dem potenziellen Opfer verbundene Kommunikationspartner oder verwendete Produkte (Supply-Chain-Angriffe)

Da Unternehmen in Baden-Württemberg gegenüber der Landesverwaltung keiner Meldepflicht in Bezug auf Cyberangriffe unterliegen, können keine belastbaren Angaben zur Gesamtzahl und Art der Angriffe auf Unternehmen gemacht werden.

Damit die künftig meldepflichtigen Stellen sich rechtzeitig auf die Meldepflichten gemäß § 4 Absatz 3 Cybersicherheitsgesetz Baden-Württemberg einstellen können, besteht die Meldepflicht gegenüber der CSBW frühestens ab dem 1. Januar 2022.

4. wie viele private Unternehmen und Behörden in Baden-Württemberg oder Behörden, Organisationen oder sonstige Einrichtungen des Landes Baden-Württemberg vom aktuellen Hackerangriff der Gruppe „REvil“ auf den IT-Dienstleister Kaseya in welchem Ausmaß jeweils mit welchen Auswirkungen betroffen sind;

Zu 4.:

Behörden, Organisationen oder sonstige Einrichtungen des Landes Baden-Württemberg waren vom Angriff der Gruppe „REvil“ auf den IT-Dienstleister Kaseya nach aktuellem Kenntnisstand nicht betroffen. Nach Kenntnisstand der Komm. ONE sind die Softwareprodukte des IT-Dienstleisters Kaseya auch im kommunalen Bereich nicht im Einsatz.

Der Polizei Baden-Württemberg liegen mit Stand vom 15. Juli 2021 Erkenntnisse zu einer einstelligen Anzahl betroffener privater Unternehmen vor. Bei den geschädigten Unternehmen wurden Teile der Firmenserver verschlüsselt, sodass es zu mehrtägigen Ausfällen von Teilen der IT-Infrastruktur kam, die erhebliche Störungen der Arbeitsabläufe sowie Folgeschäden nach sich zogen. Ersten Schätzungen eines betroffenen Unternehmens zufolge beläuft sich der finanzielle Schaden allein bei diesem Unternehmen auf einen niedrigen sechsstelligen Betrag. Zwischenzeitlich konnte bei den geschädigten Unternehmen ein Teil der betroffenen Server mittels vorhandener Backups wiederhergestellt werden.

5. welchen Handlungsbedarf und welche Möglichkeiten sie für das Land bei der Prävention im Bereich der Cybersicherheit für private Unternehmen sieht, insbesondere auch im Hinblick darauf, warum die Cybersicherheitsagentur keine ausführlichen Beratungsleistungen in diesem Sinn übernehmen soll (wie die Stellungnahme zu Ziffer 13 in Drucksache 16/9306 nahelegt);

Zu 5.:

Die zunehmende Anzahl von Cyberangriffen, die bei den betroffenen Unternehmen oftmals erhebliche Schäden anrichten, macht deutlich, dass der Prävention im Bereich Cybersicherheit eine immer größere Bedeutung zukommt. Um die Chancen der Digitalisierung wahrnehmen zu können, ist es erforderlich, dass Unternehmen rechtzeitig firmenspezifische Präventionsmaßnahmen ergreifen. Für kleine und mittlere Unternehmen besteht insbesondere der Bedarf nach niederschwelligen Präventionsangeboten, welche die Unternehmen in ihrer Umsetzung nicht überfordern aber dennoch ausreichend Schutz zur Verhinderung von Cybersicherheitsvorfällen bieten.

Über die CSBW werden künftig auch Angebote im Bereich der Prävention für Selbstständige sowie kleine und mittlere Unternehmen angeboten werden, wie dies der Koalitionsvertrag 2021 bis 2026 von BÜNDNIS 90/DIE GRÜNEN Baden-Württemberg und der CDU Baden-Württemberg explizit vorsieht.

Kleine und mittlere Unternehmen in Baden-Württemberg können bereits heute ein breites Angebot an Präventions- und Beratungsmöglichkeiten im Bereich Cybersicherheit nutzen, das unter anderem von Kammern, Wirtschaftsverbänden und IT-Netzwerken zur Verfügung gestellt wird.

So führt beispielsweise die Allianz Industrie 4.0 mit finanzieller Förderung durch das Wirtschaftsministerium vielfältige Aktivitäten durch, um insbesondere Unternehmen im verarbeitenden Gewerbe für Herausforderungen der Cybersicherheit in zunehmend vernetzten Wertschöpfungsketten zu sensibilisieren und bei der Prävention zu unterstützen. Mit der „Digitalisierungsprämie Plus“ unterstützt das Wirtschaftsministerium Unternehmen mit bis zu 500 Beschäftigten auch finanziell bei der Umsetzung von Maßnahmen zur Verbesserung der IT-Sicherheit im Betrieb. Hierzu zählen beispielsweise Investitionen in digitale IT-Sicherheitssysteme oder damit zusammenhängende Schulungen für Mitarbeitende.

Das LfV sensibilisiert anlassbezogen potenzielle Ziele mutmaßlich nachrichtendienstlich gesteuerter Cyberangriffe und bespricht hierbei präventive Maßnahmen und Handlungsempfehlungen. Im Rahmen von Vortragsveranstaltungen und mittels regelmäßiger Warnmeldungen werden zudem private Unternehmen, Verbände und öffentliche Stellen über Gefahren im Cyberbereich und über laufende Cyber-Kampagnen informiert, um die Empfänger in die Lage zu versetzen, entsprechende Angriffe rechtzeitig erkennen und abwehren zu können.

Darüber hinaus unterstützt die Polizei BW, ergänzend zu den originären polizeilichen Zuständigkeiten der Gefahrenabwehr und Strafverfolgung, bei der weitergehenden Analyse von Cyberangriffen und der Schließung von etwaigen Sicherheitslücken in betroffenen Unternehmen.

Zusätzlich stehen den Unternehmen auch entsprechende Angebote auf Bundesebene offen, etwa die vom Bundeswirtschaftsministerium geförderte „Transferstelle IT-Sicherheit im Mittelstand“, die auch regionale Anlaufstellen in Baden-Württemberg hat, oder das Förderprogramm „Go Digital“, das ein Modul zu IT-Sicherheit umfasst. Ergänzend hat die Förderung „Digital Jetzt“ u. a. eine höhere IT-Sicherheit in Unternehmen zum Ziel.

Im Übrigen wird auf die Antwort zu Ziffer 5 der Kleinen Anfrage „Cyberangriffe auf baden-württembergische Unternehmen“, Drucksache 16/7847, verwiesen.

6. welche Maßnahmen sie trifft, um Cyberangriffe auf die Durchführung der Bundestagswahlen 2021 in Baden-Württemberg zu verhindern und dadurch einen ordnungsgemäßen Verlauf von Durchführung, Auszählung und Ergebnisübertragung garantieren kann;

Zu 6.:

Hinsichtlich der Einschätzung der Gefahren und Risiken, die von möglichen Cyberangriffen auf die ordnungsgemäße Wahldurchführung ausgehen, ebenso wie hinsichtlich der bereits für die Europawahl 2019 und vor allem für die Landtagswahl 2021 umgesetzten und fortzuführenden Maßnahmen wird auf die Antwort zu Ziffer 6 des Antrags „IT-Sicherheitsvorfälle in Baden-Württemberg“, Drucksache 16/8662, verwiesen.

Über die bei der Landtagswahl 2021 auf allen Ebenen kommunizierten und umgesetzten Maßnahmen hinaus wurde zur Bundestagwahl 2021 ein nochmals deutlich erweiterter Maßnahmenkatalog von der Bundeswahlleitung zusammen mit den Landeswahlleitungen in enger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und unter Beteiligung der Sicherheitsexperten der Länder sowie unter Einbindung der kommunalen Spitzenverbände erarbeitet. Der so entstandene „Anforderungskatalog zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen – Informationssicherheit bei Schnellmeldungen“ enthält vielfältige Empfehlungen zur Umsetzung technischer und organisatorischer Maßnahmen und wurde von der Landeswahlleiterin mit Schreiben vom 1. Juni 2021 über die Kreiswahlleitungen an die Kommunen und mit Schreiben vom 7. Juni 2021 an den IT-Dienstleister Komm.ONE verteilt. Der Bundeswahlleiter steht in ständigem Austausch mit dem BSI und informiert die Landeswahlleitungen über aktuelle Entwicklungen. Die Landeswahlleiterin, die für die Vorbereitung und Durchführung der Bundestagswahl im Land zuständig ist, wird bei Fragen zu Sicherheitsaspekten in Bezug auf die anstehende Bundestagswahl durch die fachliche Expertise des Informationssicherheitsbeauftragten der Landesverwaltung (CISO), der CSBW und des Informationssicherheitsbeauftragten des Statistischen Landesamtes Baden-Württemberg unterstützt. Die Landesverwaltung steht darüber hinaus im engen Austausch mit dem BSI und erfährt auch bei der Absicherung der Bundestagswahl 2021 u. a. konkrete technische Unterstützung.

Im kommunalen Umfeld stellt der IT-Dienstleister Komm.ONE wichtige zentrale Leistungen für die Wahl zur Verfügung. Dies sind u. a. die Erstellung und der Versand der Wahlbenachrichtigungen, die Bereitstellung des Onlineantrags für Wahlscheine, die Erstellung der Wählerverzeichnisse sowie am Wahltag in einem bei Komm.ONE betriebenen System die Erfassung der Schnellmeldungen, die Berechnung und Übermittlung der Wahlergebnisse und die Ergebnispräsentation. Die Komm.ONE trifft dabei entsprechende Maßnahmen in ihrem Verantwortungsbereich, um die Sicherheit und den ordnungsgemäßen Verlauf zu gewährleisten. Dazu gehört, dass der Betrieb der zentralen Wahlanwendung im geschützten Rechenzentrum entsprechend den Anforderungen des BSI und gemäß dem zwischen Bundeswahlleitung, BSI und den Landeswahlleitungen abgestimmten umfangreichen Anforderungskatalog erfolgt. Hierzu wurden von der Komm.ONE entsprechende Sicherheits- und Datenschutzkonzepte erstellt und umgesetzt. Die Komm.ONE führt regelmäßig Tests und Überprüfungen aller wahlrelevanten Systeme durch. Aus Sicherheitsgründen können weitere Einzelheiten zu Maßnahmen nicht offengelegt werden. Zusammenfassend ist aber entsprechend den Ausführungen in Drucksache 16/8662 nochmals zu unterstreichen, dass alle mit der Wahlvorbereitung und -durchführung befassten Stellen eng zusammenarbeiten. Durch einen regelmäßigen Austausch soll die Sicherheit des Wahlablaufs gewährleistet und eine ordnungsgemäße Ermittlung des vorläufigen Wahlergebnisses sichergestellt werden. Das endgültige Wahlergebnis wird bei allen Wahlen auf allen Ebenen auf Grundlage der schriftlichen Wahlniederschriften der einzelnen Wahlorgane ermittelt.

7. welche Kenntnisse sie, insbesondere über das Landesamt für Verfassungsschutz oder die Cybersicherheitsagentur, über drohende oder durchgeführte Cyberangriffe und Manipulationen zur Einflussnahme im Zusammenhang mit der Bundestagswahl 2021 und dem dazugehörigen Wahlkampf hat;

Zu 7.:

Konkrete Kenntnisse über drohende oder durchgeführte Cyberangriffe zur Einflussnahme im Zusammenhang mit der Bundestagswahl 2021 und dem dazugehörigen Wahlkampf liegen nicht vor.

Allgemein lässt sich konstatieren, dass Desinformation und Einflussnahme bekannte Methoden fremder Mächte zur illegitimen Beeinflussung demokratischer Meinungs- und Willensbildungsprozesse sind. Sie können auch eingesetzt werden, um die Wahlaussichten von Kandidaten oder Parteien bei wichtigen Wahlen zu beeinflussen. Die Bundestagswahl ist daher ein potenziell interessantes Ziel für fremde Geheimdienste. Konkret sind zum Beispiel tendenziöse Berichterstattung in staatsnahen ausländischen Medien, „Hack and Leak“- oder „Hack and Publish“-Operationen denkbar.

Seit einiger Zeit beobachtet das LfV verstärkte Aktivitäten einer Angreifergruppierung, die unter dem Namen GHOSTWRITER bekannt geworden ist. Ihre jüngsten Angriffsversuche richteten sich vor allem gegen private E-Mail-Konten politischer Mandatsträgerinnen und Mandatsträger. Das LfV hat anlässlich dieser Phishing-Angriffswelle umfangreiche Sensibilisierungsmaßnahmen im Land eingeleitet und bereits im März 2021 politisch aktive Stellen und Personen entsprechend sensibilisiert und Handlungsempfehlungen übermittelt. Eine Intensivierung und Eskalation solcher Aktivitäten im Vorfeld der anstehenden Bundestagswahl 2021 ist nicht auszuschließen. Eine abstrakte Gefährdungslage ist somit gegeben.

8. welche Vorbereitungen und Maßnahmen sie trifft, um Angriffe und Manipulation zur Einflussnahme über soziale Medien und IT-Infrastrukturen von Bewerberinnen und Bewerbern zur Bundestagswahl 2021 sowie betroffene Parteien zu verhindern;

Zu 8.:

Bei der Bundestagswahl 2021 setzt sich die gute Kooperation der Landesverwaltung mit dem BSI konsequent fort. So wird der seitens des BSI bereits für die Landtagswahl 2021 angebotene Service der Social-Media-Account-Verifizierung für Kandidierende auch für die Bundestagswahl 2021 angeboten. Eine entsprechende Information wurde seitens der Bundeswahlleitung verteilt. Darüber hinaus hat das BSI einen „IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen“ erstellt. Darin werden den Kandidierenden konkrete Hinweise zu zentralen Themen wie der sicheren Einrichtung von Software und Geräten, dem Schutz der persönlichen Daten und der sicheren Nutzung sozialer Netzwerke dargelegt. Außerdem steht das BSI den Kandidierenden mit darin veröffentlichten Kontaktmöglichkeiten zur Seite. Der Leitfaden wurde von der Landeswahlleiterin an die Parteien zur Verteilung an die Kandidierenden versendet.

9. wie sich die Zahl der Anfragen bei der Cyberwehr seit dem Beginn der zweiten Projektphase am 1. September 2020, aufgeschlüsselt nach Monaten, entwickelt hat (auch im Vergleich zur Zeit der Pilotprojektphase);

10. zu welchen Themen diese erfolgten;

Zu 9. und 10.:

Die nachfolgende Tabelle gibt einen Überblick über das Vorfallsaufkommen und die häufigsten Ursachen. Für einzelne Monate kann aufgrund jeweils unterschiedlicher Angriffsarten keine Aussage über die häufigste Ursache getroffen werden. Insgesamt lässt sich feststellen, dass in der Vorfallsbearbeitung der Cyberwehr für den erfragten Zeitraum Ransomware als Hauptursache festgestellt wurde.

Monat	Anzahl Vorfälle	Häufigste Ursache/Angriffe	Folgen
09/2020	6	Emotet	Unbefugter Zugriff auf Daten
10/2020	6	–	–
11/2020	4	–	–
12/2020	14	Ransomware	Datenverlust, eventuell unbefugter Zugriff auf Daten mit Datenschutzverstoß
01/2021	3	–	–
02/2021	3	–	–
03/2021	21	Microsoft Exchange Schwachstelle/Hafnium	Unbefugter Zugriff auf Daten mit Datenschutzverstoß
04/2021	14	Ransomware	Datenverlust, eventuell unbefugter Zugriff auf Daten mit Datenschutzverstoß
05/2021	10	Ransomware	Datenverlust, eventuell unbefugter Zugriff auf Daten mit Datenschutzverstoß

Monat	Anzahl Vorfälle	Häufigste Ursache/Angriffe	Folgen
06/2021	13	Angriffe auf Mobilgeräte	Unbefugter Zugriff auf Daten, Missbrauch personenbezogener Daten
07/2021	8	Ransomware	Datenverlust, eventuell unbefugter Zugriff auf Daten mit Datenschutzverstoß

11. bis wann sie eine finanzielle Förderung der Cyberwehr durch das Land in welchem Umfang fortführen wird bzw. plant fortzuführen;

12. inwieweit sich die Tätigkeitsbereiche von Cyberwehr und CSBW überschneiden und insoweit zukünftig ausgestaltet werden sollen.

Zu 11. und 12.:

Die aktuelle Förderphase endet am 31. Dezember 2021. Im Übrigen wird auf die Antwort zu Ziffer 8 des Antrags „Planungen der Cybersicherheitsagentur“, Drucksache 16/9306, verwiesen.

In Vertretung

Krebs

Ministerialdirektor