Landtag von Baden-Württemberg **Drucksache 16 / 7847**

16. Wahlperiode **09. 03. 2020**

Kleine Anfrage

des Abg. Fabian Gramling CDU

und

Antwort

des Ministeriums für Inneres, Digitalisierung und Migration

Cyberangriffe auf baden-württembergische Unternehmen

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie viele Cyberangriffe gab es auf die IT von Unternehmen mit Sitz in Baden-Württemberg in den letzten drei Jahren?

2. Welche Ziele haben die Cyberangriffe jeweils verfolgt?

3. An welche Stellen können sich baden-württembergische Unternehmen im Fall von Cyberangriffen wenden?

4. Wie ermittelt die baden-württembergische Polizei in Fällen von Cyberangriffen auf Unternehmen?

5. Welche Maßnahmen ergreift die Landesregierung, um baden-württembergische Unternehmen vor Cyberangriffen zu schützen und diese zu verhindern?

06. 03. 2020

Gramling CDU

Eingegangen: 09. 03. 2020 / Ausgegeben: 08. 04. 2020

Begründung

Für Unternehmen in Baden-Württemberg wird der Schutz vor Cyberangriffen immer wichtiger. In den vergangenen Jahren haben Cyberangriffe, insbesondere auf Industrieunternehmen, in Deutschland zu Milliardenverlusten geführt. Zwar sind die Unternehmen selbst in der Pflicht, in ihre IT-Sicherheit zu investieren, allerdings bedarf es auch der Unterstützung vonseiten des Landes Baden-Württemberg.

Antwort

Mit Schreiben vom 1. April 2020 Nr. 7-0141.5/16/7847 beantwortet das Ministerium für Inneres, Digitalisierung und Migration unter Beteiligung des Ministeriums für Wirtschaft, Arbeit und Wohnungsbau die Kleine Anfrage wie folgt:

1. Wie viele Cyberangriffe gab es auf die IT von Unternehmen mit Sitz in Baden-Württemberg in den letzten drei Jahren?

Zu 1.:

Die Anzahl der Cyberangriffe auf die IT von allen Unternehmen mit Sitz in Baden-Württemberg ist nicht bekannt.

Eine Vielzahl von Angriffen wird im Übrigen von den betroffenen Unternehmen nicht oder erst nach Wochen oder Monaten bemerkt. Zudem ist hier von einem hohen Dunkelfeld auszugehen, da viele Straftaten polizeilich nicht bekannt werden, wenn beispielsweise Geschädigte einen erfolgten Cyberangriff, etwa aus Scham, aus Angst vor Reputationsverlust oder aus anderen Gründen, nicht zur Anzeige bringen.

Laut einer aktuellen Studie des Branchenverbands Bitkom e. V. waren im Zeitraum 2017 bis 2019 mindestens drei Viertel der befragten Unternehmen von digitalem oder analogem Datendiebstahl, Industriespionage oder Sabotage betroffen. Dies entspricht einem Zuwachs von 22 Prozent gegenüber den Jahren 2015 bis 2017.

2. Welche Ziele haben die Cyberangriffe jeweils verfolgt?

Zu 2.:

Grundsätzlich verfolgen Cyberangriffe eines oder mehrere von drei übergeordneten Zielen: finanzielle Bereicherung, Informationsgewinnung sowie Sabotage.

Zur Erreichung der genannten Ziele setzen die Angreifer erfahrungsgemäß insbesondere folgende Methoden ein: Ransomware, Malware, Hacking, Distributed Denial of Service (DDoS) oder Phishing. Die Aufzählung spiegelt die Häufigkeit der beschriebenen Methoden in absteigender Reihenfolge wider.

Nach Angaben der Polizei BW und des Landesamts für Verfassungsschutz Baden-Württemberg (LfV) stehen in der Mehrzahl der bekannt gewordenen Cyberangriffe eine finanzielle Bereicherung bzw. bei Cyberattacken auf Unternehmen der Spionageaspekt regelmäßig im Vordergrund. Laut LfV ist bei Cyberattacken auf Unternehmen regelmäßig Ziel der Angreifer, möglichst langfristig und unentdeckt sensible Informationen auszuspähen; teilweise sind hier entsprechende Datenabflüsse konkret nachweisbar. Zunehmend besorgniserregend sind elektronische Angriffe auf sicherheitskritische Infrastrukturen, die potenziell der Vorbereitung künftiger Sabotageaktivitäten dienen könnten. Hiervon ist aktuell besonders der Energiesektor betroffen.

Ziel dieser Angriffe waren überwiegend Unternehmen aus den Branchen Fahrzeugbau, Luft- und Raumfahrttechnik sowie der Energiebranche. Insbesondere sind vermehrt Dienstleister und Kunden von KRITIS-Betreibern in den Fokus fremder Nachrichtendienste geraten. Gerade in diesem Bereich geht das LfV von einem nicht quantifizierbaren hohen Dunkelfeld aus.

Die Motivlage der Angreifer kann in einer gewissen Anzahl von Fällen nicht mit abschließender Gewissheit festgestellt werden.

3. An welche Stellen können sich baden-württembergische Unternehmen im Fall von Cyberangriffen wenden?

Zu 3.:

In Baden-Württemberg gibt es derzeit drei Institutionen, an die sich die Wirtschaft im Fall von Cyberangriffen wenden kann. Die Polizei mit der Zentralen Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts Baden-Württemberg (LKA) und den örtlich zuständigen Polizeidienststellen, das LfV und die Cyberwehr Baden-Württemberg (Cyberwehr BW). Darüber hinaus gibt es private IT-Sicherheitsunternehmen, die betroffene Firmen bei der Behebung der Folgen von Cyberangriffen mit ihren Dienstleistungen und Produkten unterstützen können.

Die ZAC des LKA als polizeiliche Zentralstelle für Cybercrime steht rund um die Uhr als kompetenter Ansprechpartner für die Wirtschaft in allen Belangen des Themenfeldes Cybercrime zur Verfügung. Zur Kontaktaufnahme mit der Polizei, beziehungsweise zur Erstattung einer Anzeige, kommen zudem der klassische Notruf oder die Kontaktaufnahmee mit der für den Sitz des Unternehmens örtlich zuständigen Polizeidienststelle in Betracht. Dort stehen für entsprechende Fälle spezialisierte Ermittlerinnen und Ermittler bei den Kriminalinspektionen „Cybercrime und Digitale Spuren“ zur Verfügung. Auch beim LKA werden entsprechende Ermittlungen in der Fachabteilung für „Cybercrime und Digitale Spuren“ geführt.

Das LfV unterstützt betroffene Unternehmen bei der Aufarbeitung von Angriffen mit mutmaßlich nachrichtendienstlichem Hintergrund. Bei der Bearbeitung von Cyberangriffen befasst sich das LfV im Wesentlichen mit drei Hauptaufgaben: der Detektion, Attribution und Prävention. Das LfV hat dagegen keine Befugnisse, Cyberangriffe aktiv abzuwehren. Wesentlicher Teil der präventiven Aufgaben des LfV ist es, potenziell betroffene Unternehmen im Vorfeld zu warnen und zu sensibilisieren. Bei konkreten Verdachtsfällen finden anlassbezogene Sensibilisierungsgespräche mit den mutmaßlich betroffenen Unternehmen statt. Hierbei werden nach Möglichkeit technische Indikatoren des jeweiligen Angriffs übermittelt, tiefergehende Analysemöglichkeiten und Analyseparameter aufgezeigt, Angriffsvektoren beschrieben und adäquate Schutzmaßnahmen vorgeschlagen.

Insgesamt nehmen die Themenfelder Cyberspionage und Cybersabotage bei der präventiven Arbeit des LfV breiten Raum ein: Mittels zahlreicher anlassunabhängiger Beratungen und Sensibilisierungsveranstaltungen sowie über einen wöchentlichen Newsletter werden Unternehmen an die Thematik herangeführt und über Schutzmöglichkeiten informiert. Auch im Sicherheitsforum Baden-Württemberg („Sicherheitsforum Baden-Württemberg – Die Wirtschaft schützt ihr Wissen“) ist das LfV aktiv.

Die Cyberwehr BW richtet sich an kleine und mittlere Unternehmen sowie Selbstständige. Sie bietet rund um die Uhr (24/7) eine kostenlose telefonische Erstberatung und Unterstützung bei konkreten Cyberattacken. Hierfür arbeitet sie mit zertifizierten privaten IT-Sicherheitsunternehmen aus Baden-Württemberg zusammen. Zunächst wurde die Cyberwehr BW im Gebiet der Industrie- und Handelskammer (IHK) Karlsruhe als Pilotprojekt aufgebaut und seit dem Start am 1. August 2018 schon in knapp 100 Fällen kontaktiert. Der Testbetrieb der Cyberwehr BW wurde bereits evaluiert. Das Ministerium für Inneres, Digitalisierung und Migration (Innenministerium) wertet die Ergebnisse aktuell aus. Anschließend wird im Zusammenhang mit der Einrichtung der Cybersicherheitsagentur Baden-Württemberg entschieden, wie eine Ausweitung der Aktivität auf das ganze Land möglich ist. Die Möglichkeit eines niederschwelligen Angebots ohne

Strafverfolgungszwang stößt bei Betroffenen auf hohe Akzeptanz. Die Hilfe in entsprechenden Notfällen steht bei der Cyberwehr BW im Vordergrund. Gleichwohl rät die Cyberwehr BW in jedem Fall zu einer Strafanzeige bei der Polizei.

4. Wie ermittelt die baden-württembergische Polizei in Fällen von Cyberangriffen auf Unternehmen?

Zu 4.:

Die Polizei BW ergreift nach Maßgabe der einschlägigen Rechtsvorschriften die erforderlichen Maßnahmen zur Aufklärung der Straftaten, zur Ergreifung der Täterinnen und Täter sowie zur Abwehr darüber hinaus bestehender Gefahren.

In Einzelfällen wird durch die ZAC des LKA die Task Force „Digitale Spuren“ aufgerufen, durch welche erste Maßnahmen beim betroffenen Unternehmen vor Ort durchgeführt werden. Die Erstmaßnahmen erfolgen in der Regel gemeinsam mit einem beauftragten IT-Dienstleister und dienen neben beweissichernden Zwecken auch der Hilfestellung für das betroffene Unternehmen.

Bei bedeutenden Sachverhalten werden die polizeilichen Ermittlungen in Form von interdisziplinären Ermittlungsgruppen oder Besonderen Aufbauorganisationen geführt. Der personelle Ansatz liegt in diesen Fällen zum Teil über einen längeren Zeitraum im bis zu dreistelligen Bereich. Aufgrund der globalen Begehungsformen der Cybercrime werden derartige Ermittlungen in der Regel international geführt. Somit können häufig zahlreiche Unternehmen in Deutschland, aber auch global, noch rechtzeitig vor einem folgenschweren Schadenseintritt gewarnt werden.

5. Welche Maßnahmen ergreift die Landesregierung, um baden-württembergische Unternehmen vor Cyberangriffen zu schützen und diese zu verhindern?

Zu 5.:

Um seine führende Wettbewerbsposition als Hochtechnologie- und Exportland zu erhalten, muss Baden-Württemberg vor allem das wertvolle Knowhow seiner zahlreichen Weltmarktführer und seine kritischen Infrastrukturen besonders schützen. Die Landesregierung strebt zudem an, Baden-Württemberg zur digitalen Leitregion in Europa zu entwickeln. Damit Bürgerinnen und Bürger sowie Unternehmen Vertrauen in die Digitalisierung gewinnen, müssen Daten und Verbindungen sicher sein.

Vor diesem Hintergrund hat das Innenministerium die Cybersicherheitsarchitektur in Baden-Württemberg untersucht und auf Grundlage einer Organisationsanalyse die institutionalisierte Bündelung der Cybersicherheit in einer Cybersicherheitsagentur Baden-Württemberg empfohlen. Diese soll die verschiedenen Akteure zentral orchestrieren, miteinander verzahnen und dadurch einen einheitlichen Informationsfluss, eine einheitliche Strategie sowie ein abgestimmtes Handeln sicherstellen.

Für den Aufbau der Cybersicherheitsagentur Baden-Württemberg hat der Landtag von Baden-Württemberg im Haushalt für 2020/2021 insgesamt 13 Millionen Euro zur Verfügung gestellt, vor allem für 83 Personalstellen. Eine Vorbereitungsgruppe trifft aktuell die gesetzlichen, administrativen und strukturellen Vorbereitungen für den Start des Aufbaustabs.

Im Bereich der Cybersicherheit unterstützt das Land die Erforschung und Entwicklung von IT-Sicherheitstechnologien sowohl projektbezogen als auch im Rahmen der Förderung der Institute der Innovationsallianz Baden-Württemberg und der Fraunhofer-Gesellschaft.

Schwerpunkte in der IT-Sicherheit bestehen u. a. beim FZI Forschungszentrum Informatik, beim Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB), beim Fraunhofer-Institut für Produktionstechnik und Automatisierung (IPA) sowie im Institut für Mikroelektronik Stuttgart (IMS CHIPS). Diese wirtschaftsnahen Forschungseinrichtungen tragen durch die Generierung und den

Transfer von Wissen als Partner der Unternehmen für Forschung und Entwicklung und über die Qualifizierung von Fachkräften zur Stärkung des Wirtschaftsstandorts Baden-Württemberg im Bereich der IT-Sicherheit bei.

Um die Schlagkraft im Bereich der Cybersicherheit zu erhöhen, fördert das Innenministerium zudem ganz gezielt innovative Start-ups aus dem Bereich der IT-Sicherheit. Mit dem „IT-SecurityLab“ wird seit dem 1. März 2018 Start-ups aus dem Bereich IT- und Cybersicherheit zu einer schnelleren Unternehmensentwicklung verholfen. Ziel dieses Programms ist es, neue Impulse im Bereich der IT-Sicherheit zu setzen und innovative Geschäftsmodelle erfolgreich am Markt zu positionieren. So hat beispielsweise das im IT-Security-Lab entwickelte Start-up BLACKPIN aktuell im neuen baden-württembergischen Start-up-Förderprogramm den Zuschlag erhalten und wird mit einer viertel Million Euro unterstützt.

Mit der Cyberwehr BW (siehe hierzu auch Antwort auf Frage 3) beim FZI Forschungszentrum Informatik in Karlsruhe hat das Land eine professionelle Kontakt- und Beratungsstelle vor allem für kleine und mittlere Unternehmen geschaffen. Derzeit unterstützt die Cyberwehr BW ausschließlich Unternehmen in den Stadt- und Landkreisen Karlsruhe, Rastatt und Baden-Baden. Wie eine Ausweitung der Aktivität auf das ganze Land möglich ist, wird derzeit geprüft.

Die Sensibilisierung und Beratung der Wirtschaft zum Thema Cybersicherheit ist ein weiterer wichtiger Aspekt für eine erfolgreiche Digitalisierung der Wirtschaft. Mit dem vom Innenministerium organisierten und jährlich stattfindenden Cybersicherheitsforum wurde ein Forum geschaffen, um Unternehmen branchenübergreifend und kompakt über aktuelle Schwerpunktthemen der Cybersicherheit zu informieren und zu beraten. Das Cybersicherheitsforum lädt Vertreter aus Wirtschaft, Wissenschaft und Sicherheitsbehörden zum interdisziplinären Austausch ein. Impulsvorträge, Podiumsdiskussion sowie Fachpanels betrachten ein Schwerpunktthema aus unterschiedlichen Perspektiven und sind Impulsgeber für Cybersicherheit in der Wirtschaft und der Landesverwaltung. Gerade mittelständische Unternehmen sollen so für Cybersicherheit sensibilisiert werden. Über 350 Teilnehmerinnen und Teilnehmer sind der Einladung zum diesjährigen Cybersicherheitsforum gefolgt. Die Rückmeldungen aus Teilnehmerkreisen waren außergewöhnlich positiv.

Ergänzend dazu greift die Landesinformationskampagne zur Digitalisierungsstrategie „Alles beim Neuen“ das Thema Cybersicherheit auf. Unternehmer sowie deren Mitarbeiterinnen und Mitarbeiter werden damit für das Thema sensibilisiert.

Mit Investitionen in Höhe von 6,5 Millionen Euro für Anwendungen von Künstlicher Intelligenz (KI) macht das Innenministerium aktuell das LKA fit für die Zukunft. Bei der Kriminaltechnik und der Datenanalyse können mittels KI die Tatzusammenhänge schneller erkannt, Ermittlungszeiten verkürzt und Straftaten besser aufgeklärt werden.

Die Polizei BW unterstützt, 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. Darüber hinaus werden im wichtigen Bereich der Prävention relevante Hinweise und Warnmeldungen zu aktuellen Entwicklungen aus dem Bereich Cybercrime sowie zu bekannten Detektionswegen und Einfallstoren flächendeckend oder gezielt an im Einzelfall besonders gefährdete Branchen gesteuert. Dadurch sollen potentielle Opfer vor Gefahren geschützt werden.

Die ZAC des LKA initiiert, koordiniert und beteiligt sich zudem an vielfältigen Cybercrime-Kooperationen mit anderen Behörden, der Wirtschaft und der Wissenschaft auf Landes- und auf Bundesebene sowie international. Seit 2019 führt die ZAC des LKA Cyberübungen in Form von Krisenplanspielen mit Verantwortlichen der kritischen Infrastruktur des Landes durch. Diese Übungen dienen der Sensibilisierung der Teilnehmenden und der anschließenden Umsetzung von Übungserfahrungen im eigenen Betrieb. Die Resonanz auf diese Übungen ist äußerst positiv. Des Weiteren ist die ZAC des LKA bei zahlreichen Veranstaltungen von Wirtschaftsverbänden in Form von Awareness-Vorträgen beteiligt und auch auf Fachmessen präsent.

Die Stärkung der IT-Sicherheit ist eine wichtige Voraussetzung für die erfolgreiche Digitalisierung der baden-württembergischen Unternehmen und ist daher eines der zehn zentralen Handlungsfelder der „Initiative Wirtschaft 4.0 Baden-Württemberg“. Das Ministerium für Wirtschaft, Arbeit und Wohnungsbau (Wirtschaftsministerium) trägt durch verschiedene Maßnahmen zur Prävention von Cyberangriffen bei, indem es sich insbesondere für die landesweite Aufklärung und Sensibilisierung von kleinen und mittleren Unternehmen, die Förderung der anwendungsorientierten und wirtschaftsnahen Forschung sowie die Verbesserung des Wissenstransfers aus der Forschung und zwischen den Unternehmen einsetzt.

Zu diesen Maßnahmen zählt der neue Arbeitsschwerpunkt „Cybersicherheit“ der Allianz Industrie 4.0 Baden-Württemberg. In den letzten Jahren hat die Industrie hauptsächlich in die Digitalisierung der eigenen Produktion investiert. Unter der Überschrift „Industrie 4.0“ wird nun die Vernetzung über gesamte Wertschöpfungsketten forciert. Dadurch entstehen neue Möglichkeiten für Cyberangriffe. Die Allianz Industrie 4.0 Baden-Württemberg wird daher einen Schwerpunkt auf die Sensibilisierung und Wissensvermittlung zum Thema Cybersicherheit speziell im verarbeitenden Gewerbe legen.

Um die Sensibilisierung und Information von kleinen und mittleren Unternehmen zu IT-Sicherheitsfragen branchenübergreifend zu unterstützen, wurde mit finanzieller Unterstützung des Wirtschaftsministeriums das Digitale Innovationszentrum (DIZ) aufgebaut. Als gemeinschaftliche Initiative des FZI Forschungszentrums Informatik und des Unternehmensnetzwerks CyberForum e. V. bündelt das in Karlsruhe ansässige DIZ wirtschaftliche und wissenschaftliche Kompetenz im Bereich der Cybersicherheit in Baden-Württemberg. Durch das DIZ sollen aktuelle Trends und Entwicklungen in der Digitalisierung und IT-Sicherheit frühzeitig identifiziert und der Transfer sowie die Adaption neuer digitaler Technogien in die Fläche des Landes getragen werden.

Allianz Industrie 4.0 Baden-Württemberg und DIZ beteiligen sich auch intensiv an den ebenfalls vom Wirtschaftsministerium geförderten Forschungs- und Transferprojekten „CyberProtect“ und „RoboShield“ und verbreiten deren Ergebnisse und Angebote für Unternehmen flächendeckend. Diese beiden Projekte befassen sich mit der Sicherheit von Automatisierungstechnologien, der sicheren Zusammenarbeit zwischen Mensch und Roboter und dem Schutz komplexer und neuartiger Softwaresysteme für die industrielle Fertigung vor Cyberangriffen und interner Sabotage.

Ziel der Projekte ist es, einerseits Anbieter bei der Entwicklung von sicheren Produkten, Dienstleistungen und Prozessen zu unterstützen. Andererseits erhalten Anwenderunternehmen dadurch Orientierungshilfen bei der Auswahl sicherer Software und Systeme, weil für die im Rahmen dieser Projekte getesteten Produkte, Dienstleistungen und Prozesse ein Gütesiegel entwickelt wird.

Um Unternehmen eine dauerhafte Anlaufstelle für anwendungsbezogene Forschungsfragen im Bereich der Cybersicherheit zur Verfügung zu stellen, wurde zudem das mit Landesmitteln geförderte Kompetenzzentrum für IT-Sicherheit am FZI Forschungszentrum Informatik aufgebaut. Das Kompetenzzentrum unterstützt speziell kleine und mittlere Unternehmen bei der Erforschung und Entwicklung von Lösungen, wie diese die Sicherheit ihrer Produkte und Dienstleistungen gegenüber Cyberattacken erhöhen können. Im Fokus stehen hierbei neue IT-Sicherheitsherausforderungen, die sich im Zusammenhang mit dem „Internet der Dinge“, d. h. der enorm wachsenden Zahl von internetfähigen Sensoren, Geräten, Maschinen und anderen Gegenständen, ergeben.

Darüber hinaus unterstützt das Wirtschaftsministerium Unternehmen mit bis zu 100 Mitarbeitern mit der „Digitalisierungsprämie“ bei Maßnahmen zur Stärkung der IT-Sicherheit. Hierzu zählen beispielsweise Investitionen in digitale IT-Sicherheitssysteme oder damit zusammenhängende Mitarbeiterschulungen. Nach der aktuell laufenden Überarbeitung wird das Förderprogramm auch in den Jahren 2020 und 2021 weiter umgesetzt.

Ergänzend wird auf die Angebote des Sicherheitsforums Baden-Württemberg hingewiesen. Dieses unabhängige Gremium aus Unternehmen, Wissenschaft und Verwaltung des Landes Baden-Württemberg hat es sich zur Aufgabe gemacht, die heimische Wirtschaft und Forschung beim Schutz ihres Wissens und ihrer Inno-

vationen zu unterstützen. Durch den fachlichen Austausch, Veranstaltungen sowie die Veröffentlichung von Studien und Handlungsempfehlungen sollen Unternehmen über die Gefahren von Spionage und ungewolltem Knowhow-Abfluss aufgeklärt und über Möglichkeiten zu deren Abwehr informiert werden.

Strobl

Minister für Inneres,
Digitalisierung und Migration