STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Der Staatsminister

SÄCHSISCHES STAATSMINISTERIUM DES INNERN
01095 Dresden

Aktenzeichen
(bitte bei Antwort angeben)
33-1053/25/84

Dresden, 16. Mai 2017

Präsidenten des Sächsischen Landtages
Herrn Dr. Matthias Rößler
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Kleine Anfrage des Abgeordneten Sebastian Wippel, AfD-Fraktion
Drs.-Nr: 6/9360
Thema: Cyberangriffe auf Banken und Großunternehmen

Sehr geehrter Herr Präsident,

den Fragen sind folgende Ausführungen vorangestellt:

„Vorbemerkung: Laut ‚Die Welt' vom 19.04.2017 (S. 10) sollen Banken im Durchschnitt bis zu 85 Cyber-Angriffe pro Jahr ausgesetzt sein. ‚Bei jedem dritten sollen die Angreifer in irgendeiner Form Zugriff auf die Systeme der Bank erlangen', heißt es in der Tageszeitung."

Namens und im Auftrag der Sächsischen Staatsregierung beantworte ich die Kleine Anfrage wie folgt:

Frage 1:
Wie viele Banken und Großunternehmen haben in den Jahren 2014, 2015 und 2016 Cyber-Angriffe im Freistaat Sachsen zur Anzeige gebracht?

Von einer Beantwortung seitens der Staatsregierung wird abgesehen.

Gemäß Artikel 51 Absatz 1 Satz 1 der Verfassung des Freistaates Sachsen ist die Staatsregierung verpflichtet, Fragen einzelner Abgeordneter oder parlamentarische Anfragen nach bestem Wissen unverzüglich und vollständig zu beantworten. Nach dem Grundsatz der Verfassungsorgantreue ist jedes Verfassungsorgan verpflichtet, bei der Ausübung seiner Befugnisse den Funktionsbereich zu respektieren, den die hierdurch mitbetroffenen Verfassungsorgane in eigener Verantwortung wahrzunehmen haben. Dieser Grundsatz gilt zwischen der Staatsregierung und dem Parlament sowie seinen einzelnen Abgeordneten, so dass das parlamentarische Fragerecht durch die Pflicht des Abgeordneten zur Rücksichtnahme auf die Funktions- und Arbeitsfähigkeit der Staatsregierung begrenzt wird. Die Staatsregierung muss nur das mitteilen, was innerhalb der Antwortfrist mit zumutbarem Aufwand in Erfahrung gebracht werden kann (vgl. SächsVerfGH, Urteil vom 16. April 1998, Vf. 14-1-97).

Hausanschrift:
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Str. 2
01097 Dresden

Telefon +49 351 564-0
Telefax +49 351 564-3199
www.smi.sachsen.de

Verkehrsanbindung:
Zu erreichen mit den Straßenbahnlinien 3, 6, 7, 8, 13

Besucherparkplätze:
Bitte beim Empfang Wilhelm-Buck-Str. 2 oder 4 melden.

Wie viele Banken und Großunternehmen in den Jahren 2014, 2015 und 2016 Cyber-Angriffe im Freistaat Sachsen zur Anzeige gebracht haben, wird statistisch nicht erfasst. Zur vollständigen Beantwortung der Frage ist eine händische Auswertung von über 30.000 Straftaten mit dem Tatmittel Internet für die Jahre 2014 bis 2016 erforderlich. Wenn man einen Zeitansatz von 30 Minuten für die Auswertung eines Ermittlungsverfahrens ansetzt, wären dies über 15.000 Stunden für die Auswertung aller Ermittlungsverfahren. Bei einer 40-Stunden-Woche wäre ein Sachbearbeiter knapp über 375 Wochen mit dieser Auswertung befasst.

Dieses Personal stünde dann für Kernaufgaben des Polizeivollzugsdienstes nicht bzw. nur sehr eingeschränkt zur Verfügung. Die Staatsregierung kam daher bei der vorzunehmenden Abwägung zwischen dem parlamentarischen Fragerecht einerseits und der Gewährleistung der Funktionsfähigkeit der Staatsregierung sowie der ihr zugeordneten Polizeibehörden andererseits zu dem Ergebnis, dass eine Beantwortung der Frage auch unter Berücksichtigung des hohen Rangs des parlamentarischen Fragerechts unverhältnismäßig und ohne erhebliche Einschränkung der Funktionsfähigkeit der sächsischen Polizei nicht zu leisten ist.

Frage 2:
Welche Erkenntnisse über die tatsächliche Zahl von schwerwiegenden Cyberangriffen auf Banken und Großbetriebe hat die Sächsische Staatsregierung?

Eine Definition für „schwerwiegende" Cyberangriffe als Grundlage für eine statistische Erhebung liegt nicht vor. Im Rahmen des IT-Sicherheitsgesetzes des Bundes ist seit dem 3. Mai 2016 eine Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Kritisverordnung) in Kraft, die für die vier KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung gilt. Weitere Sektoren sollen kurzfristig geregelt werden. Die als KRITIS eingestuften Unternehmen der ersten vier Sektoren mussten demnach bis zum 3. November 2016 dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Kontaktstelle im Unternehmen melden, die bei IT-Sicherheitsvorfällen vom BSI gewarnt wird oder das BSI bei eigenen Vorfällen zu informieren hat. Diese Meldungen werden dann je nach Standort der KRITIS an die zuständigen Aufsichtsbehörden der Länder übermittelt. Im Zeitraum vom 3. November bis 31. Dezember 2016 wurde in diesem Rahmen keiner Aufsichtsbehörde im Freistaat Sachsen ein Sicherheitsvorfall eines in Sachsen beheimateten KRITIS-Unternehmen übermittelt. Eine darüber hinausgehende Meldestruktur, die Unternehmen im Sinne der Fragestellung verpflichtet, Cyber-Angriffe zu melden bzw. anzuzeigen, besteht nicht.

Frage 3:
Welche unterstützenden Maßnahmen bietet der Freistaat Sachsen Banken und Großunternehmen an, um a) Cyber-Angriffe besser abwehren zu können und b) auf erfolgte Cyber-Angriffe zu reagieren, um einen bestmöglichen Datenschutz für die Kunden zu gewährleisten?

Das Landeskriminalamt Sachsen (LKA) unterstützt im Rahmen des Präventionsangebotes „Sicheres Unternehmen" sächsische klein- und mittelständische Unternehmen (KMU) auf Grundlage eines ganzheitlichen Sicherheitskonzeptes. Dies geschieht insbesondere durch eine Sensibilisierung der Unternehmen für die Themen Wirtschaftskriminalität, Wirtschafts- und Industriespionage, um mögliche Sicherheitsrisiken zu er-

kennen und diese durch geeignete Gegenmaßnahmen möglichst nachhaltig zu beseitigen. Die Empfehlungen des LKA schließen Maßnahmen zur IT-Sicherheit und Bekämpfung von Cyber-Angriffen ein. Die Komplexität von Banken und Großunternehmen im Freistaat Sachsen macht es notwendig, diese auf die Angebote des BSI zu verweisen.

Im Rahmen seiner gesetzlich zugewiesenen Aufgaben informiert, sensibilisiert und berät das Landesamt für Verfassungsschutz (LfV) Sachsen Unternehmen, öffentliche Stellen und interessierte Bürger durch Tagungen, Vorträge, Pressemitteilungen und Einzelgesprächen zu den Möglichkeiten der Prävention gegen elektronische Angriffe. So hatte beispielsweise das LfV Sachsen am 21. September 2016 gemeinsam mit der Sächsischen Industrie- und Handelskammer zu einem gemeinsamen Wirtschaftsschutztag zum Thema „Spionageabwehr in Wirtschaft und Wissenschaft" eingeladen.

Banken und Großunternehmen sind in der Regel professionell gegen Cyberattacken aufgestellt. Der Freistaat Sachsen bietet unterstützende Maßnahmen gegen Cyberangriffe deshalb vor allem den KMU an. So hat der Beauftragte für Informationssicherheit des Landes im Jahr 2016 mehrere Vorträge zu Abwehr- und Reaktionsmaßnahmen vor Unternehmen gehalten und zusammen mit der Industrie- und Handelskammer und der Handwerkskammer Dresden eine Sensibilisierungsveranstaltung für die KMU im Rahmen der Strategie „Sachsen Digital" zur IT-Sicherheit organisiert, die unter der Federführung des Sächsischen Staatsministeriums für Wirtschaft, Arbeit und Verkehr erstellt und weiterentwickelt wird.

Im Rahmen des Förderprogramms „Verbesserung des Informationssicherheitsniveaus in KMU" der Mittelstandsrichtlinie werden Unternehmen dabei unterstützt, vorhandene Engpässe und Lücken des eigenen Schutzniveaus vornehmlich in der digitalen Vernetzung innerhalb und außerhalb von Organisationen zu erkennen sowie geeignete Maßnahmen im Zuge einer stringenten Schutzstrategie abzuleiten. Im Zusammenhang mit der Einführung bzw. der Zertifizierung eines Informationsmanagementsystems nach ISO/IEC 27001 oder eines alternativen Systems werden u. a. Ausgaben zur Schulung von Mitarbeitern, Beratungsleistungen durch qualifizierte Dienstleister sowie der Erwerb spezieller Software finanziell unterstützt.

Frage 4:
Werden Banken und Unternehmen eigene Erkenntnisse des Freistaates Sachsen zur Erhöhung der IT-Sicherheit proaktiv zur Verfügung gestellt, z.B. Erkenntnisse, die aufgrund von Angriffen auf Behörden gewonnen wurden?

Die Verfassungsschutzämter der Länder und des Bundes erstellen anlassbezogen Analysen und Handlungsempfehlungen zu bekanntgewordenen elektronischen Angriffen. Diese Analysen und Handlungsempfehlungen werden dann in anonymisierter Form an potentiell Betroffene zur Verfügung gestellt. Zugleich wird angeboten, weiter unterstützend tätig zu werden.

Erkenntnisse über Angriffsvektoren werden bei dem im Staatsbetrieb Sächsische Informatik Dienste (SID) ansässigen Sächsischen Computer Emergency Response Team (SAX.CERT) gesammelt und koordiniert. Das SAX.CERT ist dabei formell nur für die Behörden des Freistaates Sachsen zuständig. Das SAX.CERT ist jedoch auch Mitglied im Verbund der deutschen CERTs (CERT-Verbund), in dem neben den jeweiligen

Bundes- bzw. Landes-CERT u. a. große Firmen aller Wirtschaftsbereiche und Universitäten Mitglied sind. In den genannten Gremien erfolgt ein aktiver Austausch von Informationen, die dazu beitragen können, die Sicherheit der Mitglieder zu verbessern.

Frage 5:
Wie erfolgt der Austausch im Falle von Cyber-Angriffen mit dem Verfassungsschutz? Wie ist das Landesamt hierbei eingebunden?

Der Austausch von Informationen erfolgt im Sinne der Fragestellung nach den maßgeblichen Rechtsvorschriften des Sächsischen Verfassungsschutzgesetzes (SächsVSG). So können gemäß § 10 Abs. 1 SächsVSG die Behörden und Gerichte des Freistaates Sachsen, die Gemeinden, Landkreise und sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts von sich aus dem LfV Sachsen die ihnen bekannt gewordenen personenbezogenen Daten und sonstigen Informationen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Informationen u. a. zur Wahrnehmung von Aufgaben nach § 2 Abs. 1 Nr. 2 SächsVSG erforderlich sind.

Mit freundlichen Grüßen

Markus Ulbig