STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Der Staatsminister

SÄCHSISCHES STAATSMINISTERIUM DES INNERN
01095 Dresden

Geschäftszeichen
(bitte bei Antwort angeben)
16-0141-50/

Dresden, 8. April 2022

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

Kleine Anfrage des Abgeordneten Carsten Hütter (AfD)
Drs.-Nr.: 7/ 9368
Thema: Wirtschaftsspionage im Freistaat Sachsen

Sehr geehrter Herr Präsident,

den Fragen sind folgende Ausführungen vorangestellt:

„Der Präsident des Bundesamtes für Verfassungsschutz Haldenwang wird in der ‚Wirtschaftswoche', Ausgabe 3 vom 14.01.2022, wie folgt zitiert: ‚Wir haben Anhaltspunkte, dass Cyberkriminelle direkt im Auftrag fremder Nachrichtendienste arbeiten. Etwa, dass sie Daten, die sie bei ihren Attacken erbeutet haben, an staatliche Stellen weitergeben oder verkaufen' und ‚die Grenzen zwischen kriminellen Hackern und staatlichen oder halbstaatlichen ausländischen Stellen verschwimmen'."

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

Frage 1:
Welche Erkenntnisse hat die Staatsregierung zum Umfang und der Art von Wirtschaftsspionage (auch versuchter Spionage) ausländischer Staaten in Sachsen – sowohl via Internet/Funk als auch analog?

Frage 2:
Welche Erkenntnisse hat die Staatsregierung insbesondere zu der Frage, wie viele staatliche Stellen und Unternehmen, welcher Branchen, in Sachsen in den Jahren 2020, 2021 sowie 2022 bis zum aktuellen Zeitpunkt Opfer von Wirtschaftsspionage geworden sind und welche Auswirkungen diese ggf. hatte? (Bitte aufschlüsseln nach Geschädigten/Betroffenen Unternehmen und staatlichen Stellen und nach verursachten Schäden [bspw. durch Schadsoftware] bzw. Wertigkeiten von erlangten Informationen soweit beziffer-/schätzbar sowie Ursprung/Herkunft der Angriffe)

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.

Frage 3:
Welche Erkenntnisse hat die Staatsregierung insbesondere zur Zusammenarbeit von staatlichen oder halbstaatlichen ausländischen Stellen und „privaten" Hackern/Cyberkriminellen und Größenordnungen von Geldern, die für den Verkauf/ Kauf von erbeuteten Daten fließen/flossen?

Zusammenfassende Antwort auf die Fragen 1 bis 3:

Die Staatsregierung hat keine Erkenntnisse im Sinne der Fragestellungen.

Frage 4:
Welche Anstrengungen (in sachlicher und personeller Hinsicht) unternimmt der Freistaat Sachsen, um sächsische Unternehmen vor Wirtschaftsspionage zu schützen? (Bitte jährliche aufschlüsseln für die Jahre seit 2015 nach personeller und sachlicher Ausstattung und Behörde)

Wesentliche Aspekte, sächsische Unternehmen vor Wirtschaftsspionage zu schützen, sind das Sensibilisieren zu diesem Phänomen und das Ausprägen eines entsprechenden Sicherheitsbewusstseins sowohl bei der Unternehmensführung als auch den Mitarbeiterinnen und Mitarbeitern.

Das Präventionsangebot „Sicheres Unternehmen", das im Jahr 2012 landesweit eingerichtet wurde, dient dem Ziel der Verbesserung der Sicherheit sächsischer Unternehmen. Zielgruppe sind insbesondere Klein- und Mittelständische Unternehmen. Ein Bestandteil des Präventionsangebotes ist u. a. eine Beratung bezüglich einer Spionage- und Proliferationsrelevanz. Vor diesem Hintergrund war neben dem Sächsischen Verband für Sicherheit in der Wirtschaft e. V. (seit 2017 Allianz für Sicherheit in der Wirtschaft Sachsen e. V.) auch das Landesamt für Verfassungsschutz (LfV) Sachsen ein Kooperationspartner für die Umsetzung des Präventionsangebotes.

Die Schwerpunkte des ganzheitlichen Beratungsangebotes liegen dabei auf Objektsicherheit, Personal- und Organisationssicherheit sowie Cybercrime. Mit einem initialen Sicherheits-Check erhalten die Unternehmen eine umfassende Analyse zum Sicherheitsstatus und zu bestehenden Sicherheitslücken. Auf dieser Grundlage erarbeiten kompetente Fachberater des Präventionsangebotes „Sicheres Unternehmen" Sicherheitsempfehlungen, die auf die Anforderungen der Unternehmen zugeschnitten sind.

Es ist jedoch darauf hinzuweisen, dass die im Rahmen des Präventionsangebotes durchgeführten Beratungen insbesondere die materielle Sicherheit (Einbruchschutz) sowie teilweise die IT-Sicherheit der Unternehmen zum Gegenstand hatten. Das Thema „Spionage und Proliferation" besaß bei den beratenen Unternehmen hingegen keine Relevanz. Angaben zur personellen Ausstattung im Sachzusammenhang werden statistisch nicht erfasst. Insofern kann hierzu keine Aussage getroffen werden.

Das LfV Sachsen fungiert dabei als lokaler Sicherheits- und Ansprechpartner für sächsische Unternehmen, um diese beim Schutz vor Wirtschaftsspionage zu unterstützen. Das LfV Sachsen geht zu diesem Zweck aktiv auf potenziell gefährdete Unternehmen zu. Als Bestandteil einer Sicherheitspartnerschaft kommen grundsätzlich Vorträge, individuelle Beratungen oder auch der Versand von Broschüren in Betracht. Die vertrauliche Behand-

lung der jeweiligen Sicherheitspartnerschaft und ihres Inhaltes ist dabei selbstverständlich. Bedingt durch die Corona-Pandemie konnte das LfV Sachsen seit 2020 nur sehr wenige Vorträge und individuelle Beratungen durchführen. Stattdessen legte das LfV Sachsen den Schwerpunkt seiner Arbeit darauf, Unternehmen mittels anlassbezogener Rundschreiben zu Informationen über aktuelle elektronische Angriffskampagnen, verbunden mit konkreten Handreichungen für Abwehrmaßnahmen, zu sensibilisieren.

Im Rahmen der Mittelstandsrichtlinie als Teil der E-Business-Förderung bietet der Freistaat Sachsen den Unternehmen die Möglichkeit, eine Förderung für den Bereich Informationsschutz (Informationssicherheit) zu beantragen.

Diese Förderung soll dazu beitragen, den Schutz der Informationen und IT-Systeme zu verbessern beziehungsweise zu gewährleisten und den Informationsschutz konzeptionell vorzubereiten.

Folgende Maßnahmen werden hier konkret unterstützt:

- Schutzbedarfsfeststellung
  Beratungen durch qualifizierte IT-Dienstleister zur Schutzbedarfsfeststellung im Unternehmen, zur Analyse schutzrelevanter Unternehmensprozesse und zur Ableitung von Handlungsempfehlungen auf Basis ISO 27001 beziehungsweise der jeweiligen branchenspezifischen IT-Sicherheitsstandards oder ähnlich anerkannter Standards wie BSI-Grundschutz (IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik).
- Umsetzung der Handlungsempfehlungen
  - Beratungen zur Umsetzung der infolge identifizierter, unternehmenskritischer Anwendungen erforderlichen zugeordneten Schutzmaßnahmen,
  - Neuerwerb projektspezifischer Hard- und Software,
  - Einführung in die betriebliche Praxis einschließlich technischer Anbindung und Schulung.

Hierfür wurden in der EFRE-Förderperiode 2014 bis 2020 folgende Mittel zur Verfügung gestellt:

Jahr	**EFRE-Finanzplan (Stand 25.01.2022) in Mio. €**
2015	6,84
2016	6,98
2017	5,3
2018	8,06
2019	19,18
2020	7,5

Auch in der Förderperiode 2021 bis 2027 werden hierfür Mittel zur Verfügung stehen; die finanzielle Ausstattung ist noch nicht abschließend festgelegt.

„IT- und Cybersicherheit gewährleisten" ist ein wichtiges strategisches Ziel in der ressortübergreifenden Strategie „Sachsen Digital". Erpressungstrojaner, manipulierte Smartphones, virtueller Identitätsdiebstahl: Werden Sicherheitsrisiken nicht erkannt, können Cyberangriffe für Unternehmen schnell zum wirtschaftlichen Aus führen. Auf der Agenda der Betriebe sollte das Thema deshalb ganz oben stehen – schon bevor der erste Angriff erfolgt.

Diesem präventiven Ansatz folgend, hat das Staatsministerium für Wirtschaft, Arbeit und Verkehr im Rahmen von „Sachsen Digital" in den Jahren 2017 und 2018 eine Veranstaltungsreihe zum Thema „IT-Sicherheit" für sächsische Unternehmen in Kooperation mit den sächsischen Industrie- und Handelskammern sowie den Handwerkskammern durchgeführt.

In kompakten Veranstaltungen erfuhren Geschäftsführer, Betriebsleiter und IT-Entscheider, was zu tun ist: Wo liegen die größten Risiken? Wie werden Mitarbeiterinnen und Mitarbeiter am besten sensibilisiert? Handlungsbedarfe und wichtige Rechtsgrundlagen wurden ebenso vermittelt wie Unterstützungsmöglichkeiten und Förderprogramme zum Thema.

Die Veranstaltungen waren jeweils gezielt auf die Bedürfnisse von Händlern, produzierenden Unternehmen und Dienstleistern ausgerichtet.

Frage 5:
In wie vielen erkannten/aufgedeckten Spionagefällen wurden Verfahren wegen des Cyberangriffs/Spionage, insbesondere Strafverfahren, geführt und wie oft wandten sich sächsische Behörden an jene anderer Bundesländer und anderer Staaten und wie häufig war diese Zusammenarbeit erfolgreich? (Bitte jährlich aufschlüsseln für die Jahre 2020, 2021 sowie 2022 bis zum aktuellen Zeitpunkt)

Bei den sächsischen Staatsanwaltschaften sind keine Ermittlungsverfahren bekannt, in denen Daten im Auftrag fremder Staaten oder fremder Nachrichtendienste ausspioniert wurden. Soweit Ermittlungsverfahren wegen des Tatverdachts des Ausspähens von Daten über das Internet zu Lasten von sächsischen Wirtschaftsunternehmen geführt wurden, gab es in diesen Verfahren keine Anhaltspunkte für eine Zusammenarbeit der Täter mit ausländischen Staaten beziehungsweise für eine gezielte Weiterleitung der ausgespähten Daten an staatliche oder halbstaatliche ausländische Stellen.

Mit freundlichen Grüßen

Prof. Dr. Roland Wöller