SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 20/3942**
20. Wahlperiode 6. Februar 2026

Kleine Anfrage

des Abgeordneten Kianusch Stender (SPD)

und Antwort

der Landesregierung – Ministerin für Inneres, Kommunales, Wohnen und Sport (MIKWS)

Cyberangriffe auf Unternehmen in Schleswig-Holstein

Cyberangriffe stellen für Unternehmen ein zunehmendes Risiko dar. Neben möglichen Betriebsunterbrechungen können erhebliche wirtschaftliche Schäden entstehen, die insbesondere kleine und mittlere Unternehmen stark belasten können.

Vorbemerkung der Landesregierung:

Es wird darauf hingewiesen, dass der Begriff „Cyberangriff“ kein fest definierter polizeilicher Fachbegriff ist. Im polizeilichen Kontext ist dieser Begriff daher auslegungsbedürftig. Darunter ist grundsätzlich jeder vorsätzliche, unbefugte Eingriff in IT-Systeme zu fassen, bei dem Daten gestohlen, manipuliert, gestört oder zerstört oder Funktionen beeinträchtigt werden sollen. Häufig wird unter einem Cyberangriff allerdings lediglich ein sogenannter Ransomware-Angriff verstanden. Daneben existieren jedoch zahlreiche weitere Erscheinungsformen von Angriffen im Cyberraum, wie beispielsweise Distributed-Denial-of-Service-(DDoS)-Angriffe, Angriffe im Rahmen von Business-E-Mail-Compromise (BEC), Phishing-Angriffe sowie weitere Varianten. Die nachfolgenden Ausführungen beziehen sich auf den Phänomenbereich Ransomware.

1. Welche Erkenntnisse liegen der Landesregierung zu der Anzahl von Cyberangriffen auf Unternehmen in Schleswig-Holstein in den Jahren 2024 und 2025 vor?

   Antwort:

   Die statistischen Fallzahlen unterliegen grundsätzlich Veränderungen, da insbesondere im Bereich der Ransomware bekannt gewordene Fälle auch zeitverzögert durch Ermittlungen oder Nachmeldungen in die polizeiliche Statistik einfließen können. Zudem ist von einem relevanten Dunkelfeld auszugehen, da nicht jedes betroffene Unternehmen einen Ransomware-Angriff zur Anzeige bringt.

   Im polizeilichen Hellfeld liegen für das Jahr 2024 in Schleswig-Holstein derzeit 27 bekannt gewordene Fälle vor, bei denen privatwirtschaftliche Unternehmen betroffen waren. Für das Jahr 2025 sind bislang 29 entsprechende Fälle bekannt geworden.

   Im Cyberraum werden täglich und in großer Zahl Angriffe ausgeführt. Das BKA geht davon aus, dass mehr als 68% der Unternehmen von Cyberangriffen betroffen sind, die Tendenz ist steigend.

2. Welche Branchen oder Unternehmensgrößen waren nach Kenntnis der Landesregierung besonders häufig betroffen?

   Antwort:

   Auf Grundlage der vorliegenden Daten kann nicht festgestellt werden, dass bestimmte Branchen in besonderem Maße von Ransomware-Angriffen betroffen sind. Die Auswahl der Tatobjekte erfolgt nach polizeilicher Einschätzung überwiegend zufällig. Dabei zeigen die bisherigen Erkenntnisse , dass die Täter in der Regel solche Unternehmen angreifen, bei denen eine verwertbare Sicherheitslücke in den IT-Systemen besteht. Gezielte Angriffe auf bestimmte Branchen oder Unternehmen sind im Bereich der Ransomware nach derzeitiger Erkenntnislage nicht feststellbar.

3. Welche Informationen hat die Landesregierung über die wirtschaftlichen bzw. finanziellen Schäden, die Unternehmen in Schleswig-Holstein durch Cyberangriffe in den Jahren 2024 und 2025 entstanden sind?

Antwort:

Der Landespolizei liegen keine eigenen belastbaren Zahlen vor. Erfasst werden Erpressungsforderungen sowie gegebenenfalls gezahlte Beträge.

4. Welche Formen der Unterstützung – finanziell oder nicht finanziell – bietet das Land Schleswig-Holstein Unternehmen an, die von Cyberangriffen betroffen sind?

   Antwort:

   Es erfolgt eine Sensibilisierung der Unternehmen und ein Austausch in Form von Veranstaltungen (inkl. Praxisbericht eines betroffenen Unternehmens) wie bspw. ,,Gemeinsam sicher: IT-Security für Schleswig -Holsteins Wirtschaft" im März 2025 (Gemeinsame Veranstaltung MWVATT und der SicherheitsPartnerschaft Schleswig-Holstein, bestehend aus dem Ministerium für Inneres, Kommunales, Wohnen und Sport des Landes Schleswig-Holstein, der Allianz für Sicherheit in der Wirtschaft Norddeutschland e.V. (ASWN), des Digitale Wirtschaft Schleswig-Holstein e.V. (DiWiSH) und der IHK Schleswig-Holstein).

   Das vom MWVATT geförderte Cluster DiWiSH hat in den letzten Jahren zudem mehrfach betroffene Unternehmen an passende IT Sicherheitsunternehmen weitervermittelt.

   Weiterhin sind im Rahmen der Förderung innovativer Digitalisierungsmaßnahmen in kleinen Unternehmen (DKU) Vorhaben förderfähig, die darauf ausgerichtet sind, bestehende betriebliche Abläufe und Prozesse umfassend auf Innovationspotenziale durch Digitalisierung zu analysieren sowie dafür geeignete individuelle Lösungen und Handlungsempfehlungen zu entwickeln. Diese dienen der Verbesserung der IT-Sicherheit oder der Verbesserung digitaler Geschäftsmodelle oder der Digitalisierung von Prozessen oder der Digitalisierung von Produkten und Verfahren.

5. In welchem Umfang wurden diese Unterstützungsangebote in den Jahren 2024 und 2025 in Anspruch genommen?

   Antwort:

   Dazu liegen keine konkreten Zahlen vor. Das Cluster DiWiSH hat mehrfach betroffene Unternehmen an passende IT Sicherheitsunternehmen vermittelt.

6. Plant die Landesregierung angesichts der aktuellen Gefährdungslage eine Ausweitung oder Weiterentwicklung bestehender Unterstützungsprogramme für Unternehmen im Bereich IT-Sicherheit oder Cyberresilienz?

   Antwort:

   Das MWVATT plant die Förderung eines Projektes „SicherDigital.SH: Cybersicherheit in KMU - Stärkung der IT und Informationssicherheit in der Wirtschaft Schleswig-Holsteins“ und schafft damit eine dringend benötigte Anlaufstelle, um kleine und mittlere Unternehmen bei der Bewältigung wachsender Cyberrisiken und der Umsetzung von NIS2-Pflichten praxisnah zu unterstützen und zu sensibilisieren. Das im Cluster DiWiSH angesiedeltes Projekt soll die Sensibilisierung und Durchführung von Maßnahmen bei den Unternehmen forcieren. Damit leistet das Projekt einen wertvollen Beitrag zur Erhöhung der IT-Resilienz der schleswig-holsteinischen Wirtschaft und trägt zur Umsetzung der Digitalstrategie des Landes bei.

7. Welche Maßnahmen ergreift das Land, um insbesondere kleine und mittlere Unternehmen präventiv über Cybergefahren, Sicherheitsstandards und Handlungsempfehlungen zu informieren?

   Antwort:

   In Schleswig-Holstein ist bei der Landespolizei insbesondere die Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt (LKA) für die Präventionsarbeit zuständig. Die ZAC hält regelmäßig Vorträge für Verbände sowie für einzelne Unternehmen, wobei häufig kleine und mittlere Unternehmen adressiert werden. In Zusammenarbeit mit der Industrie- und Handelskammer werden Krisensimulationsworkshops angeboten, in denen ein Cyberangriff in Form eines Rollenspiels durchgespielt wird.

   Die Landespolizei ist Teil einer Sicherheitspartnerschaft mit der IHK, der Allianz für Sicherheit in der Wirtschaft Norddeutschland e.V. (ASWN) sowie der Digitalen Wirtschaft Schleswig-Holstein. Im Rahmen dieser Partnerschaft finden Informationsveranstaltungen, Messeauftritte und weitere Formate zur Sensibilisierung für Cybercrime statt.

   Ergänzend dazu veröffentlicht die Landespolizei Pressemitteilungen zu Cybercrime-Themen und gibt bei aktuellen oder branchenspezifischen Bedrohungslagen gezielte Warnmeldungen heraus (zuletzt z. B. für das Hotelgewerbe). Die ZAC steht zudem in regelmäßigem Austausch mit

Akteuren wie dem CERT-Nord und dem ressortübergreifenden Informationssicherheitsmanagement der Staatskanzlei sowie mit dem Verfassungsschutz zum Themenfeld Wirtschaftsschutz.

Die Verfassungsschutzbehörde arbeitet präventiv durch Aufklärung mit Unternehmen, Behörden und Forschungseinrichtungen zusammen, indem zu den Gefahren durch ausländische Nachrichtendienste im Cyberbereich sensibilisiert wird. Dies geschieht beispielsweise über direkte Kontakte mit den Bedarfsträgern (sowohl proaktiv als auch auf Nachfrage) sowie im Rahmen der Sicherheitspartnerschaft zusammen mit weiteren Behörden und Verbänden, darunter der Polizei und der IHK.