SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 20/4480**
20. Wahlperiode 08. Juni 2026

Kleine Anfrage

des Abgeordneten Kianusch Stender (SPD)

und Antwort

der Landesregierung – Der Minister und Chef der Staatskanzlei

Cyberkriminalität - Cyberangriffe gegenüber der Landesverwaltung

Vorbemerkung

Für die IT-Systeme und Arbeitsplätze der Landesverwaltung ist eine defensive, auf Trennung ausgelegte Sicherheitsarchitektur implementiert. Eine direkte Anbindung an das Internet besteht nicht, sodass Nutzende und die Systeme keine unkontrollierten direkten Verbindungen in das Internet aufbauen können und von dort auch nicht sichtbar und somit auch nicht direkt erreichbar sind (vgl. dazu auch Umdruck 20/4680).

Die Begrifflichkeit „Cyberangriff“ unterliegt keiner Legaldefinition und wird im Hinblick auf die Fragestellung als Straftat im engeren Sinne ausgelegt. Dieses umfasst gemäß des in der Landespolizei angewendeten Konzeptes zur Bekämpfung der Cybercrime folgende Delikte:

- ausspähen / abfangen von Daten (sowie Vorbereitungshandlungen)
- betreiben krimineller Handelsplattformen
- Datenhehlerei
- Fälschung beweiserheblicher Daten
- Täuschung im Rechtsverkehr bei Datenverarbeitung
- Datenveränderung

- Computersabotage (oftmals i.V.m. Erpressung)

Es wird polizeilicherseits ein Dunkelfeld angenommen. Oftmals verbleiben Taten, besonders im Phänomenbereich des Phishings, im Stadium des Versuchs und werden aufgrund dessen nicht zur Anzeige gebracht bzw. gemeldet.

1. Wie viele Cyberangriffe bzw. sicherheitsrelevante IT-Vorfälle auf Einrichtungen der Schleswig-Holsteinischen Landesverwaltung wurden seit Beginn der 20. Legislaturperiode registriert? Bitte detailliert auflisten nach Jahr, Landesbehörde und Beeinträchtigung durch den Angriff (tatsächliche Ausfälle, Einschränkungen des Verwaltungsbetriebs, finanzieller Schaden).

   Die Darstellung erfolgt direkt in der Tabelle in der Anlage. Monetäre Schäden im engeren Sinne wurden seit Beginn der 20. Legislaturperiode nicht registriert.

2. Zu Frage 1: Welche Arten von Angriffen wurden hierbei festgestellt? Bitte differenzieren nach Malware, Phishing, Ransomware, DDoS-Angriffen, unbefugten Zugriffsversuchen, Datenabfluss, etc.

   Die Darstellung erfolgt direkt in der Tabelle in der Anlage.

3. In welchen Fällen waren personenbezogene Daten betroffen / potenziell betroffen?

   Die Darstellung erfolgt direkt in der Tabelle in der Anlage.

   Sofern personenbezogen Daten (potenziell) betroffen sind, erfolgen ergänzend entsprechende Meldungen an das ULD.

   Im Regelfall kann bei Ransomwaredelikten eine mindestens potenzielle Betroffenheit von personenbezogenen Daten angenommen werden.

4. Welche Erkenntnisse liegen der Landesregierung über die Herkunft welcher Angriffe vor?

   Besonders hinsichtlich der DDoS-Angriffe bekennen sich überwiegend Gruppierungen wie „NoName057(16)“ und „Overflame“ zu den Taten. Diese Gruppierungen sind häufig politisch motiviert („hacktivistisches Kollektiv“) und handeln mutmaßlich als Unterstützer der Russischen Föderation im Kontext des völkerrechtswidrigen Angriffs Russlands auf die Ukraine, häufig als Reaktion auf aktuelle politische Entscheidungen. Die registrierten Ransomwaredelikte können in der Mehrzahl auf bekannte Gruppierungen wie zum Beispiel „Royal“ und „Phobos“ zurückgeführt werden. Die Herkunft vieler Ransomwaregruppierungen lässt sich nur bedingt eindeutig feststellen, da die Täter ihre Identität bewusst verschleiern. Überwiegend können diese

Gruppierungen Regionen wie Osteuropa und Russland zugeordnet werden. Aber auch in Asien, Lateinamerika und weiteren Regionen nimmt die internationale Vernetzung im Cybercrime-Bereich zu. Darüber hinaus verdichten sich Hinweise, dass die Täter aus Ländern heraus, in denen die Strafverfolgung nur eingeschränkt erfolgt oder die internationale Zusammenarbeit schwierig ist, operieren. Einige Gruppierungen vermeiden Angriffe auf Systeme in ihren mutmaßlichen Herkunftsländern.

5. Liegen der Landesregierung Erkenntnisse über Cyberangriffe oder sonstige sicherheitsrelevante IT-Vorfälle bei Kommunen und Kreisen im Land in den Jahren 2022 bis bislang 2026 vor? Wenn ja, welche mit welcher Beeinträchtigung (tatsächliche Ausfälle, Einschränkungen des Verwaltungsbetriebs, finanzieller Schaden)?

   Die Cybersicherheit der Kommunen und das einschlägige Vorfallsmanagement liegt nicht in der Verantwortung des Landes, sondern wird vielmehr im Rahmen der kommunalen Selbstverwaltung eigenständig ausgeübt. Gleichwohl gibt es zahlreiche Angebote des Landes, welche den Kommunen durch das Land zur Mitnutzung zur Verfügung gestellt wurden, so z.B. das CERT Nord (Computer Emergency Response Team) sowie die die mobilen Security Incident Response Teams, welche im Schadenfall Detektion und Wiederherstellung übernehmen können.

   Sofern der Landesregierung Erkenntnisse über Cyberangriffe auf die Kommunen vorliegen, sind diese ebenfalls in der Anlage aufgeführt.

Jahr	Land / Kommune	Meldende Behörde / ggf. Verfahren	Art	Anzahl	Schaden / Auswirkung
2022	Land	Staatskanzlei / Landesportal	DDoS	1	Temporärer Ausfall Landesportal
2022	Land	Staatskanzlei / digitales.sh	Unbefugter Zugriffsversuch	1	Keine
2022	Land	MBWK	DDoS	1	Temporärer Ausfall Schulportal
2022	Land	Staatskanzlei / digitales.sh	Kompromittierungsversuch	1	Keine
2022	Land	LKA Cybercrime	Ransomware / Verschlüsselung	2	Keine / begrenzt
2022	Land	LKA Cybercrime	Phising	2	Keine / begrenzt
2022	Land	LKA Cybercrime	Diverses*	7	Keine / begrenzt
2022	Kommunal	Zweckverband Ostholstein	Schadcodefund nach Übertragung von Daten zu Dataport	1	Keine
2023	Land	Staatskanzlei / Landesportal	DDoS	2	Temporärer Ausfall Landesportal
2023	Land	Staatskanzlei	Phisingversuch	2	Keine
2023	Land	GMSH	Verdacht auf Quakbot Infektion	1	Keine
2023	Land	Landwirtschaftskammer	Verdacht auf Quakbot Infektion	1	Keine
2023	Land	MJG / Justizportal	DDoS	1	Temporärer Ausfall Justizportal
2023	Land	FM / Data Boreum	Abgewehrte Malware	44	Keine
2023	Land	MBWK	Unautorisierte Systemnutzung	1	IS-Propaganda-Video auf Digitaler Tafel an Schule Achter de Weiden, Schenefeld

2023	Land	LKA Cybercrime	Ransomware / Verschlüsselung	4	Keine / begrenzt
2023	Land	LKA Cybercrime	DDoS	1	Keine / begrenzt
2023	Land	LKA Cybercrime	Phising	1	Keine / begrenzt
2023	Land	LKA Cybercrime	Diverses*	5	Keine / begrenzt
2023	Kommunal	Kreis Dithmarschen	Erfolgreiches Phising	1	Abfluss Benutzerdaten
2023	Kommunal	Übergreifend / Bürgerportal SH	Systemausfälle durch Bot "thesis-research-bot"	1	Temporärer Ausfall Bürgerportal SH
2024	Land	Staatskanzlei	Phisingversuch	2	Keine
2024	Land	Staatskanzlei / Landesportal	DDoS	2	Temporärer Ausfall Landesportal
2024	Land	MIKWS	Phising	1	Potenziell Abfluss von Nutzerdaten Potenzielle Datenschutzrelevanz
2024	Land	MIKWS	Phisingversuch	2	Keine
2024	Land	LasD	Phisingversuch	1	Keine
2024	Land	MEKUN	Phising-Kampagne	1	Potenziell Abfluss von Nutzerdaten Potenzielle Datenschutzrelevanz
2024	Land	LKA Cybercrime	Ransomware / Verschlüsselung	1	Keine / begrenzt
2024	Land	LKA Cybercrime	DDoS	3	Keine / begrenzt
2024	Land	LKA Cybercrime	Phishing	0	-
2024	Land	LKA Cybercrime	Diverses*	3	Keine / begrenzt

2024	Kommunal	Kreis Dithmarschen	Phischingversuch	1	Keine
2024	Kommunal	Hansestadt Lübeck	DDoS	1	Temporärer Ausfall von lübeck.de
2025	Land	MEKUN	Phisingversuch	1	Keine
2025	Land	Staatskanzlei / Landesportal	DDoS auf RSS-Feeder beim Landesportal_SH	1	Temporärer Ausfall des RSS-Feed
2025	Land	MJG	Unautorisierte Systemnutzung / Unbekannte Remote Assistance Anfragen	1	Keine
2025	Land	Staatskanzlei / OpenXChange	Abgewehrte Malware	1	Keine
2025	Land	Staatskanzlei / Landesportal	DDoS	3	Keine
2025	Land	MIKWS	Phishing	1	Potenziell Abfluss von Nutzerdaten Potenzielle Datenschutzrelevanz
2025	Land	MIKWS	Fake-Telefonat / Vortäuschung fremder Identität	1	Keine
2025	Land	LVGEO	Erfolgreiche Installation eines Schadprogramms (Malware Epibrowser)	1	Keine
2025	Land	MJG	Erfolgreiche Installation eines Schadprogramms (Malware Epibrowser)	1	Keine
2025	Land	Landtag	Phisingversuch	1	Keine
2025	Land	MIKWS	Phisingversuch	1	Keine

2025	Land	Staatskanzlei / Landesportal	Unautorisierte Systemnutzung / Massenhafter Versand von Spam über die Kontaktformulare des Landesportals SH	1	begrenzt
2025	Land	LKA Cybercrime	Ransomware / Verschlüsselung	0	-
2025	Land	LKA Cybercrime	DDoS	8	Keine / begrenzt
2025	Land	LKA Cybercrime	Phishing	0	-
2025	Land	LKA Cybercrime	Diverses*	2	Keine / begrenzt
2025	Kommunal	Kreis Ostholstein	DDoS	3	Keine
2025	Kommunal	Zweckverband Ostholstein	Kompromittierte Zugangsdaten / Installation eines Schadprogramms	1	begrenzt
2025	Kommunal	Kreis Dithmarschen	Phisingversuch	1	Keine
2025	Kommunal	Stadt Kiel	DDoS	2	Temporärer Ausfall von kiel.de
2025	Kommunal	Kreis Nordfriesland	DDoS	1	Temporärer Ausfall von norfriesland.de
2025	Kommunal	Kreis Nordfriesland	DDoS	1	Keine
2026	Land	u.a. UKSH	Cyberangriff auf einen externen Dienstleister diverser Krankenhäuser	1	Noch in Behandlung Abfluss von Patientendaten; Datenschutzrelevanz
2026	Land	MIKWS	Phisingversuch	2	Keine
2026	Land	FM (Steuerverwaltung)	Phishing Angriff auf Dataport und die 6 Steuerverwaltungen der ndL	1	Potenziell Abfluss von Nutzerdaten Potenzielle Datenschutzrelevanz
2026	Land	MWVAT	Versuchte SQL Injection auf BOB-SH über das Kontaktformular	1	Keine

2026	Kommunal	Stadt Schwentinental	Phishing-Kampagne	1	Potenziell Abfluss von Nutzerdaten Potenzielle Datenschutzrelevanz
2026	Kommunal	Kreis Ostholstein	DDoS	1	Keine
2026	Kommunal	Stadt Schenefeld	Phising	1	Potenziell Abfluss von Nutzerdaten Potenzielle Datenschutzrelevanz

*umfasst z. B. Malware, Sextortion, sowie Auffälligkeiten wie möglichen Datenabfluss oder auffällige IP-Adressen.