Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

Wirtschafts- und Digitalisierungs-
ausschuss
des Schleswig-Holsteinischen Landtages

nur per E-Mail: Wirtschaftsausschuss@landtag.ltsh.de

Landesbeauftragte für Datenschutz
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Frau Dr. h. c. Hansen
Durchwahl: 988-1200

Aktenzeichen:
LD3-50.12/24.001

Kiel, 11.11.2024

Schleswig-Holsteinischer Landtag
Umdruck 20/3940

Zum Bericht über die Cybersicherheit unserer Infrastruktur, LT-Drs. 20/1584
TOP 1, 31. Sitzung des Wirtschafts- und Digitalisierungsausschusses am 13.11.2024

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für die Gelegenheit zur Stellungnahme zum Bericht der Landesregierung „Bericht über die Cybersicherheit unserer Infrastruktur" (LT-Drs. 20/1584 vom 07.11.2023).

Mir als Datenschutzaufsichtsbehörde sind in Schleswig-Holstein „Verletzungen des Schutzes personenbezogener Daten" (so genannte „Datenpannen") zu melden. Dies umfasst Meldungen aus öffentlichen und nichtöffentlichen Stellen (gemäß Artikel 33 DSGVO, § 41 LDSG oder § 65 BDSG i.V.m. § 500 StPO).

Im vergangenen Jahr sind 527 Meldungen bei meiner Dienststelle eingegangen (siehe auch mein 42. Tätigkeitsbericht, Abschnitt 1.2, https://www.datenschutzzentrum.de/tb/tb42/kap01.html#12).
Zwar betreffen diese Meldungen nur Verletzungen im Bereich der Verarbeitung *personenbezogener* Daten und daher nicht sämtliche Verletzungen der Informationssicherheit, doch lassen sich aus den Meldungen einige Schlüsse auch in Bezug auf den Zustand der Cybersicherheit ziehen:

Zum einen erfolgen Datenschutzverletzungen aufgrund fehlerhafter Bedienung (z. B. falsch zugewiesene Zugriffsrechte) oder menschlichen Fehlverhaltens (Fehlversand von E-Mails durch Auswahl eines falschen Empfängers, Fehlkuvertierung von Briefen, Fehlablage in Dateisystemen und Akten) oder mangelnder Vorgaben und mangelnder Sensibilisierung. Diese sind nicht einem aktiven Angreifer zuzuordnen.

Zum anderen lässt sich eine nicht unerhebliche Anzahl von Datenschutzverletzungen auf Angriffe zurückführen, die insbesondere durch Schadsoftware und Phishing mit dem Ziel, IT-Systeme unbefugt zu benutzen (z. B. zu unbefugtem Versand von E-Mails) oder den Zugriff auf

Daten bis zu einer Lösegeldzahlung zu verwehren (z. B. durch Verschlüsselungstrojaner), durchgeführt werden. Dies geht mit einem unbefugten Zugriff auf Daten einher: Beispielsweise erlaubt die Erlangung eines E-Mail-Passworts nicht nur den Versand von Spam und anderen unerwünschten Nachrichten, sondern den Zugriff auf die gesamte gespeicherte E-Mail-Korrespondenz, und dies kann wiederum (etwas durch Formulierung von authentisch wirkenden Phishing-E-Mails) zum Angriff auf Dritte genutzt werden kann. Häufig ließen sich solche Angriffe abwehren – sei es durch das rechtzeitige Einspielen von **Sicherheitsupdates** und **Verwendung aktueller Softwareversionen** oder durch die Nutzung von **Sicherheitsfunktionalitäten** (z .B. Zwei-Faktor-Authentisierung, Geräte-Authentisierungen, Einschränkung auf bestimmte Netze), wie sie z. B. im Bereich des Online-Bankings mittlerweile üblich sind.

Dies führt zu der Beobachtung, dass neben dem Datenschutz auch die Informationssicherheit häufig **nur unzureichend koordiniert** und nicht ganzheitlich und nachhaltig behandelt wird. Dies ist jedoch für ein angemessenes Schutzniveau erforderlich, denn für einen erfolgreichen Angriff reicht **eine Sicherheitslücke** aus, während es eine verlässliche Abwehr gegen mögliche Angriffe erfordert, **sämtliche Sicherheitslücken** zu schließen.

Ein geeignetes Vorgehen zur Stärkung der Informationssicherheit besteht darin, insbesondere auf Landes- und Kommunalebene, **gemeinsam Standards der Informationssicherheit umzusetzen**. Die Herausforderung dabei ist, gleichartige Sachverhalte (z. B. die Absicherung von Arbeitsplatz-Rechnern) einheitlich zu behandeln und eine Standardisierung stringent durchzusetzen, zugleich aber genügend Raum für die spezifischen Besonderheiten der Behörden zu lassen. So hat beispielsweise der Landesbetrieb für Küstenschutz, Nationalpark und Meeresschutz bei der Steuerung der Sielentwässerung andere Aspekte zu beachten als eine Ministerialverwaltung oder ein Stadtteilbüro einer Kommune mit Publikumsverkehr.

Auf Landesebene gibt es mit dem **zentralen Sicherheitsmanagement** (CISO, AG ISMS, vgl. Abschnitt 3.8.1 des Berichts) im Prinzip eine geeignete Organisationsstruktur, doch ist diese nach unserer Wahrnehmung derzeit noch nicht mit **hinreichenden Ressourcen** ausgestattet: Zwar gibt es eine Vielzahl von Sicherheitsmaßnahmen, aber deren nach Möglichkeit standardisierte Gestaltung und Dokumentation sowie deren Überprüfung von Vollständigkeit und Wirksamkeit sind nicht immer gewährleistet. Probleme bereiten neben einer notwendigen Fortbildung auch häufige Personalwechsel, wenn das Querschnittsthema Informationssicherheit nicht kontinuierlich durch eingearbeitete Teams bearbeitet werden kann, zumal die notwendigen Lern- und Einarbeitungsprozesse Zeit in Anspruch nehmen. Schließlich ist es wichtig, dass Informationssicherheit wegen der Breitenwirkung und Wichtigkeit für die Organisation als **zentrale Aufgabe** verstanden wird und dementsprechend organisatorisch auf geeignete Weise, z. B. als Stabsstelle, eingebunden ist. Die in Abschnitt 3.8.1.1 des Berichts formulierten Anforderungen sollten daher, wo noch nichterfolgt, stringent umgesetzt werden. Dies gilt in ähnlicher Weise auch auf der kommunale Ebene.

Aus **technischer Sicht** ist zu beobachten, dass Angriffe bevorzugt auf weit verbreitete Soft- und Hardwarekomponenten erfolgen, da etablierte Angriffsmuster auf diese Weise mehrfach eingesetzt werden können. Ebenso wirksam sind Angriffe auf Zentralsysteme, die weltweit Steuerungsfunktionen haben oder auf diese einwirken, z. B. „Supply-Chain-Angriffe", bei denen über Systeme von Lieferanten schadhafte Software an deren Kunden verbreitet werden. Aber nicht nur Schadcode, sondern auch fehlerhafte Software kann eine Vielzahl von Geräten und Organisationen treffen und diese sogar arbeitsunfähig machen – etwa bei der automatisierten Auslieferung einer fehlerhafte Komponente einer Sicherheitssoftware, die weltweit zahlreiche Arbeitsplatzrechner in zahlreichen Organisationen, wozu auch das UKSH zählte, sperrte (vgl. https://www.uksh.de/Service/Presse/Presseinformationen/2024/Nach+globalem+IT_Ausfall_+UKSH+wieder+im+Normalbetrieb-p-218229.html)

Daher ist der Ansatz der Landesregierung, die Nutzung alternativer Soft- und Hardwarekomponenten voranzutreiben und **auf Basis von Open-Source eine souveräne Datenverarbeitung** mit eigener Steuerungsmöglichkeit anzustreben, zu begrüßen. Zwar stellen sich ebenfalls Herausforderungen in der Integration und Nutzung von Open-Source-Komponenten, doch dürften die Einfluss- und Steuerungsmöglichkeiten des Landes dabei deutlich größer sein im Vergleich zu einer Bindung an einen einzelnen weltweit agierenden Anbieter. In solchen Fällen sind auch weitere mögliche Auswirkungen der Abhängigkeiten zu betrachten, beispielsweise dadurch, dass eine politische Einflussnahme Dritter auf solche Anbieter nicht ausgeschlossen werden kann.

Generell gilt es für jede Organisation und auch für das Land Schleswig-Holstein in der Konzeption und im Betrieb von Informationstechnik, sich aller **bestehenden Abhängigkeiten** bewusst zu werden und Maßnahmen zu treffen, damit sich diese nach Möglichkeit nicht negativ auswirken können. Insoweit kann es in einigen Bereichen auch notwendig sein, redundante Komponenten vorzusehen und auf eine etwas heterogenere Gestaltung der IT-Landschaft anstelle von Monokulturen zu setzen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat unter meinem Vorsitz im Jahr 2023 ein Positionspapier zu Kriterien für Souveräne Clouds vorgelegt, in dem auf die in der Datenschutz-Grundverordnung niedergelegten **Anforderungen an Sicherheit wie Effektivität, Nachprüfbarkeit und Dauerhaftigkeit** insbesondere in Bezug auf etwaige Abhängigkeiten eingegangen wird, abrufbar unter https://uldsh.de/dsk-souvclouds (siehe auch meinen 42. Tätigkeitsbericht, Abschnitt 6.2.4, https://www.datenschutzzentrum.de/tb/tb42/kap06.html#624). Eine Orientierung an diesen Anforderungen für eine souveräne Sicherheit – entsprechend dem zu gewährleistenden Schutzniveau und dem jeweils mit der Verarbeitung verbundenen Risiko – ist auch für die Verarbeitung von Daten ohne Personenbezug gerade im öffentlichen Bereich empfohlen.

Für Nachfragen stehen Ihnen mein Team und ich gern zur Verfügung.

Mit freundlichen Grüßen

gez. Dr. h. c. Marit Hansen
Landesbeauftragte für Datenschutz