Schleswig-Holstein
Der echte Norden

echtdigital
Vernetzt mit der Zukunft

SH
Schleswig-Holstein
Der Chef der Staatskanzlei

Der Chef der Staatskanzlei | Postfach 7122 | 24171 Kiel

Vorsitzender des Wirtschafts- und
Digitalisierungsausschusses
Claus Christian Claussen
Landeshaus
24105 Kiel

Minister

Schleswig-Holsteinischer Landtag
Umdruck 20/4680

02. April 2025

Sachstand Informationssicherheit Landesverwaltung

Sehr geehrter Herr Vorsitzender,

mit Drucksache 20/1584 hat die Landesregierung auf Antrag des SSW (Drucksache 20/797) einen „Bericht über die Cybersicherheit unserer Infrastruktur" abgegeben. In der 43. Sitzung des Wirtschafts- und Digitalisierungsausschusses am 4.Dezember 2024 wurden seitens der StK ergänzende Informationen zum Sachstand der Informationssicherheit in der Landesverwaltung dargestellt, um offene Fragen des Ausschusses insbesondere aus den Anhörungen zu Drucksache 20/1584 zu beantworten. Die Staatskanzlei wurde gebeten, diese Informationen zusammenzufassen und schriftlich einen aktuellen Sachstand zu den Aktivitäten der Landesregierung zu geben.

Ausgangssituation

Wie bereits schriftlich im Bericht und mündlich in den Sitzungen dargestellt hat sich die Lage der Informationssicherheit der öffentlichen Verwaltung in den letzten Jahren deutlich verändert.

Länder und Kommunen sind zunehmend Ziel auch gerichteter Angriffe. Neben eher als digitalen „Vandalismus" zu kategorisierenden Angriffen auf die Verfügbarkeit von öffentlichen Auftritten der Landesverwaltung sind vermehrt auch gezielte Angriffe mit (wirtschafts-)kriminellen Hintergründen deutlich auf dem Vormarsch. Nicht zuletzt durch den Angriffskrieg Russlands steigt auch die Anzahl der politisch motivierten Angriffe auf die öffentliche Verwaltung. Gleichzeitig fällt es zunehmend schwer, das notwendige Fachpersonal zu finden, Stellenbesetzungsverfahren verlaufen teilweise ergebnislos. Dies erschwert die Umsetzung der von der Landesregierung ergriffenen Maßnahmen in verschiedenen Bereichen, auf die im Folgenden detailliert eingegangen wird.

Architektur

Die Landesverwaltung Schleswig-Holstein ist mit einer sehr defensiven, auf Trennung ausgerichteten Architektur auch für die kommenden Jahre gut aufgestellt. Durch die weitestgehende Verlagerung der Datenverarbeitung auf den mit mehreren Ländern gemeinsam eingerichteten IT-Dienstleister Dataport kann ein andauernd hohes Sicherheitsniveau gehalten werden. Ein verwaltungseigener Betrieb durch die Ministerien und nachgeordneten Bereiche ist nur noch in Ausnahmefällen mit Blick auf die engen Personalressourcen sinnvoll und in der Regel hinsichtlich der umfangreichen Investitionen des Landes zur Informationssicherheit bei Dataport häufig nicht wirtschaftlich. Dataport betreibt eigene Rechenzentren mit gedoppelten Infrastrukturen und hohem Aufwand für Resilienz und Unabhängigkeit von Dritten. Dataport setzt die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik um und ist wiederholt durch das BSI zertifiziert worden. Der Betrieb von IT durch Landesdienststellen ist aus Sicht der Staatskanzlei nicht zielführend, operative Tätigkeiten im Bereich der IT auf Ebene der Landesverwaltung sind sowohl aus Gründen der Informationssicherheit als auch mit Blick auf die ohnehin engen Personalressourcen bereits kurzfristig keine sinnvolle und vertretbare Option.

Die Landesverwaltung ist nicht direkt an das Internet angebunden. Systeme der Landesverwaltung können grundsätzlich keine direkte, unkontrollierte Verbindung ins Internet aufbauen und sind von dort auch nicht erreichbar. Die Landesverwaltung greift nur über zusätzliche Sicherheitssysteme wie Firewalls und Proxies auf das Internet zu. Inhalte aus dem Internet werden insbesondere im Bereich E-Mails, aber z. B. auch bei Antragsdaten über OZG-Dienste auf Schadsoftware gescannt. Sowohl auf Ebene der Architektur als auch in der Umsetzung im Betrieb ist die Landesverwaltung durch Separierung und Isolation auf infrastrukturelle und dauerhafte Sicherheit ausgelegt. Dies ist mit hohem Aufwand und merklichen Einschränkungen verbunden.

Die Verarbeitung kritischer Daten und der Betrieb von Systemen mit hohen Verfügbarkeitsanforderungen erfolgt in der Landesverwaltung strikt getrennt von den Systemen der allgemeinen Bürokommunikation, die der dominierende Eingangsvektor für die Angriffe auf unsere Infrastruktur sind. Administrative Zugriffe auf kritische Daten und Systeme erfolgen bei Dataport aus besonders gesicherten Umgebungen und werden vollständig überwacht. Ein direkter Datenaustausch ist auch für die Fachadministration bei Dataport nicht möglich. Externe wie beispielsweise Personal der Hersteller oder Beratungsunternehmen erhalten keinen direkten Zugriff auf die Systeme.

Die Vernetzung der verschiedenen Dienststellen der Kommunen und der Landesverwaltung erfolgt über das Landesnetz Schleswig-Holstein. Das Landesnetz ist ein vom Internet komplett getrenntes Netz auf Basis eigens hierfür angemieteter Glasfaserleitungen regional ansässiger Glasfaseranbieter. Der Betrieb und die Administration des Netzes erfolgt durch Dataport.

Informationssicherheitsmanagement

Um die Anforderungen an die Informationssicherheit gleichmäßig zu steuern und einheitlich weiterzuentwickeln, sind in der Staatskanzlei, den Ministerien und den nachgeordneten Bereichen Informationssicherheitsbeauftragte benannt, die sich schwerpunktmäßig um die korrekte Abwicklung dieser Verfahren mit Dataport und um ressortspezifische Sicherheitsfragen kümmern. Zu jedem Verfahren und zu jeder

Infrastruktur beschäftigt Dataport Informationsicherheitskoordinatoren, die den Betrieb nach Vorgaben des BSI IT-Grundschutzes ausrichten.

Die Staatskanzlei hat in den letzten Monaten eine Reorganisation des zentralen IT-Managements durchgeführt und hierbei insbesondere ein eigenes Referat ausgeprägt, in dem die Themen des Informationssicherheitsmangements und der IT-Notfallvorsorge zentral ausgebaut und fortlaufend koordiniert werden. Die Rolle CISO wurde inklusive Stellvertretung neu besetzt und sowohl enger in die Führungsorganisation eingebunden als auch mit den verantwortlichen Bereichen für die zentralen Dienste und Systeme stärker vernetzt. Das Team wird durch weitere Personen in operativen Fragen ergänzt und greift seinerseits auf umfangreiche Dienstleistungen bei Dataport zu.

Informationssicherheit ist in vielen Bereichen neben der technisch-operativen Umsetzung auch ein richtlinien- und nachweisorientierter Prozess, der auf Basis der nationalen Standards des BSI durchaus hohen administrativen Aufwand verursacht. Seitens der Staatskanzlei wird für die Ressorts ein zentrales Unterstützungssystem vorgehalten, um diese Arbeiten zu erleichtern. Das System mit dem Namen HiScout wird zentral betrieben und ermöglicht eine elektronische und teil-automatisierte Bearbeitung der notwendigen Sicherheitskonzepte und Nachweise. Für die Koordination in der Bearbeitung von Sicherheitsvorfällen und -problemen wird die Staatskanzlei das bereits vorhandene ITIL-konforme Steuerungssystem ITSM-SH/ assyst auf den Bereich der Informationssicherheit ausweiten. Bisher wird ITSM-SH/ assyst bereits für die Koordination und Steuerung von Fragen zum Betrieb der Informations- und Kommunikationssysteme eingesetzt.

Kooperation

Gemeinsam mit Hamburg, Bremen und Sachsen-Anhalt betreibt die Landesregierung ein Computer Emergency Response Team (CERT Nord). Das CERT Nord nimmt übergreifende Aufgaben in diesem Länderverbund wahr, zu den Aufgaben gehören unter anderem der Betrieb von Informations-, Warn- und Alarmdiensten, die Beratung in IT-Sicherheitsfragen, die Behandlung von Sicherheitsvorfällen und Berichtserstellung sowie die Schnittstelle zu externen Organisationen wie dem BSI und dem Verbund aller Verwaltungs-CERTs in Deutschland.

Das CERT Nord war ursprünglich nur für die Landesverwaltung eingerichtet, konnte aber in den letzten Jahren im Zuge der Amtshilfe auch durch die Kommunalverwaltung in Schleswig-Holstein genutzt werden. Die Verträge mit dem CERT Nord sind seitens Sachsen-Anhalt und Schleswig-Holstein seit 2024 so erweitert worden, dass nun auch alle Kommunen die Informationen und Dienstleistungen des CERT Nord erhalten können. Darüber hinaus wurden gemeinsam mit Sachsen-Anhalt gesonderte Verträge (xIRT) über Dataport geschlossen, die in Fällen tatsächlich auftretender Sicherheitsvorfälle, die zur Einschränkung / zum Ausfall von IT-Systemen führen, Teams bereitstellen, die sowohl vor Ort als virtuell (remote) Detektion und Wiederherstellung der Betriebsbereitschaft sicherstellen. Diese zentralen Koordinierungs- und Unterstützungsleistungen werden durch die Landesregierung finanziert und den Kommunen kostenfrei zur Verfügung gestellt. Dies stellt eine wesentliche Entlastung der kommunalen Ebene in der übergreifenden Koordinierung von Informationssicherheitsfragen dar. Die Landesregierung ermöglicht hiermit eine zentrale Einbindung der Kommunen in den Gesamtverbund der Cybersicherheit in Deutschland.

Das CERT Nord stellt im Zuge der KRITIS-Betreuung diese Informationen und Dienstleistungen auch der Privatwirtschaft zur Verfügung.

In bisherigen Fällen erfolgreicher Angriffen auf die Privatwirtschaft hat die Landesregierung sowohl die Dienstleistungen des CERT Nord als auch weiterer Dataport-Experten als direkte Hilfe angeboten.

In besonderen Situationen werden die Servicezeiten erweitert und zusätzliche Sicherheitsteams bereitgestellt. So wurden in der Schlussphase der Bundestagswahl sowohl im Bereich Informationssicherheit als auch im Bereich des IT-Betriebs zusätzliche Unterstützungsleistungen erbracht. Durch diesen Einsatz konnte die Vorbereitung der Wahl und der Wahlabend in Fragen der Informationssicherheit und des Betriebs gut unterstützt werden.

Die Landesverwaltung steht mit dem BSI seit längerer Zeit in Verhandlungen zu einer vertieften Kooperation über die bereits bei und über Dataport bestehende intensive Zusammenarbeit hinaus. Das BSI kann hier nur auf Basis konkreter Kooperationsverträge tätig werden. Die Kooperationsfelder sind momentan durch verfassungsrechtliche Vorgaben des Bundesinnenministeriums beschränkt auf allgemeine Beratungs- und Unterstützungsthemen. Gemeinsame Aufgabenerledigung und auch eine Aufgabenverlagerung sind nach Rechtsauffassung des BMI aktuell wegen fehlender rechtlicher Grundlagen und verfasssungsrechtlicher Grenzen nicht möglich.

Die Landesregierung setzt sich dafür ein, mit dem BSI auch die aus Sicht Schleswig-Holsteins zielführenden Kooperationsfelder eines gemeinsamen Krisenmanagements, gemeinsamer Lagebilder und gemeinsamer Werkzeuge voranzutreiben. In einem ersten Schritt wird die Landesregierung in den Bereichen des Informationsaustausches, von Schulung und Sensibilisierungen sowie besonderer Beratungsangebote auch für die lokale Wirtschaft mit dem BSI kooperieren. Hierzu wird auf Seiten des BSI und des BMI zum aktuellen Zeitpunkt ein Kooperationsvertrag abgestimmt. Aktuell gehen BSI und die hier federführend für das Land verhandelnde Staatskanzlei davon aus, dass im zweiten Quartal die Kooperationsvereinbarung unterzeichnet werden kann. Unabhängig davon steht das Land mit dem BSI weiterhin in direktem Austausch und wird beispielsweise auch an einer gemeinsamen Cybersicherheitsübung Anfang April teilnehmen.

NIS-2

Mit der NIS-2-Richtlinie hat die europäische Union einen wesentlichen Schritt zum Etablieren eines vergleichbaren Sicherheitsniveaus und harmonisierten Vorgehens zur Informationssicherheit eingeleitet. Durch die langjährige Orientierung an den Standards und Vorgehensweisen des BSI auf Landesebene, aber insbesondere auch wegen der umfassenden Verlagerung der operativen IT auf Dataport sind die notwendigen Voraussetzungen zur Umsetzung bereits geschaffen.

Während die Grunderwägungen der NIS-2-Richtlinie weitestgehend deckungsgleich zu den in der Landesverwaltung bereits bestehenden Vorgaben sind, besteht aus Sicht der Staatskanzlei Anpassungsbedarf in einzelnen Regelungen. Um den Nachweis einer richtlinienkonformen Ausgestaltung der Informationssicherheit in der Landesverwaltung zu erleichtern und gleichzeitig die nicht mehr vor der Bundestagswahl beschlossenen Umsetzungsideen des Bundes zu berücksichtigen, wird als erster Schritt die bestehende Leitlinie auf Landesebene angepasst werden.

Die Staatskanzlei wird unabhängig von der NIS-2-Umsetzung auf Ebene der Länder und des Bundes mit den Kommunen in Schleswig-Holstein erörtern, wie durch ein Informationssicherheitsgesetz auf Landesebene eine besseren Koordination, Einheitlichkeit und auch kooperative und synergetische Umsetzung erreicht werden kann.

Unterstützung für Kommunen

Auch wenn die Kommunen in Fragen der Informationssicherheit selbstständig und auch eigenverantwortlich sind, ergibt es aus Sicht des Landes Sinn, die im Bereich der Umsetzung des Onlinezugangsgesetz und auch in der Nachnutzung der vom Land zentral bereitgestellten Infrastrukturen bereits bestehende ebenenübergreifende Kooperation und fortlaufende projekthaft vorangetriebene Harmonisierung auch im Bereich der Informationssicherheit fortzuentwickeln. Das Land stellt aus diesem Grund umfangreiche Unterstützung sowohl in Fragen des Informationssicherheitsmanagements als auch der konkreten Umsetzung zur Verfügung.

Für den Aufbau eines Sicherheitsmanagements in den Kommunen stellt das Land seit Jahren ein kommunal angepasstes Vorgehen bereit, welches auch regelmäßig mit dem ITVSH abgestimmt wird. Unter dem Namen „SiKoSH" hat sich mittlerweile ein Vorgehen etabliert, mit dem Kommunen einfach und geordnet ihr Sicherheitsmanagement erweitern können. Dies wird fortlaufend und gerade aktuell auch an die geänderten Standards und Vorgehensweisen des BSI angepasst.

Wie auch für die Landesverwaltung ist es aus Sicht des Landes für viele Kommunen der beste Weg, die dargestellten Landesinfrastrukturen einfach mit- und nachzunutzen. Die Kommunen profitieren in diesem Fällen direkt von den Vorarbeiten und laufenden Aufwänden, die ohnehin für die Landesverwaltung anfallen. Es gibt einige Kommunen, die den Landesstandard +1 einsetzen, sich ausschließlich über das sichere Landesnetz mit dem Internet verbinden und den Betrieb ihrer kommunalen Fachverfahren auf den Dienstleister Dataport verlagern, deren „Miteigentümer" sie als kommunale Träger sind. Diese weitestgehende Verlagerung operativer Fragen auf kommunale Dienstleister wird seitens des Landes aus hierfür bereitgestellten Harmonisierungsmitteln projekthaft unterstützt.

Gleichzeitig investiert das Land auch in übergreifende Sicherheitsmaßnahmen, um die Kommunen zu entlasten. Beispielsweise stehen an allen Schulen kostenfrei sichere Internetzugänge über das glasfaserbasierte Landesnetz zur Verfügung. An zentraler Stelle betreibt das Land für die Kommunen eine auf die pädagogische Nutzung angepasste Firewallinfrastruktur. Die Schulträger müssen sich hier nicht um die aufwändige Absicherung kümmern.

Modernisierung

Die Landesverwaltung modernisiert aktuell die Arbeitsplatzinfrastrukturen. In anderem Zusammenhang und mit Blick auf das Gewährleisten von Digitaler Souveränität und Offener Innovation wird über dieses Vorgehen bereits umfassend informiert. Neben der Umstellung der wesentlichen Komponenten auf Open Source findet in diesem Zuge auch eine zusätzliche Härtung der neuen Systeme und eine Anpassung an die neuen Sicherheitsherausforderungen statt.

Für das Landesportal werden neben zusätzlichen Schutzmaßnahmen zur Abwehr von massenhaften Angriffen auch die Infrastrukturen selbst an die geänderten Anforderungen angepasst. Gerade im Zeitalter von zunehmender Desinformation kommt staatlich bereitgestellten Informationsplattformen eine deutlich wichtigere Rolle zu. Das Landesportal wird aktuell auf eine neue Open Source-Software umgestellt und gleichzeitig in ein Betriebsmodell überführt, in dem selbst Hochlastszenarien während eines Angriffs

ohne weitere Eingriffe bewältigen werden können. Diese Arbeitsergebnisse stehen auch allen anderen Anwender:innen zur Verfügung und wirken gleichzeitig sowohl für das Landesportal als auch für die vom Land finanzierten und gemeinsam mit dem ITVSH betriebenen Bürgerportale der Kommunen

Für über das Internet erreichbare Dienste wird zunächst für das Land, nachfolgend aber auch für die Kommunen ein vom BSI empfohlener, zentraler Schwachstellenscanner eingerichtet, der kostenfrei nutzbar sein wird. Zusätzlich wird im Landesnetz die interne Sensorik zur Angriffserkennung und -nachverfolgung ausgeweitet.

Mit freundlichen Grüßen

Dirk Schrödter