2. Strategisches Ziel: Informations- und Cybersicherheit gewährleisten

2. Strategisches Ziel: Informations- und Cybersicherheit gewährleisten

Die Menschen nutzen heutzutage ganz selbstverständlich zahlreiche Anwendungen auf ihren digitalen Endgeräten und verbinden ihre Gebrauchsgegenstände zunehmend mit dem Internet. Die Unternehmen produzieren nicht nur immer mehr vernetzte Gebrauchsgegenstände, sondern setzen auch bei ihrer internen Organisation auf eine neue Dimension der Vernetzung, die ihren Ausdruck im Schlagwort „Wirtschaft 4.0" findet. Und schließlich verwendet auch die öffentliche Verwaltung zunehmend auf Informationstechnik (IT) gestützte Verfahren.

Aufgrund der zunehmenden digitalen Vernetzung aller Lebensbereiche gewinnt die Informations- und Cybersicherheit immens an Bedeutung. Ziel des Freistaates Sachsen ist es, den Ursachen für Sicherheitsvorfälle entgegenzuwirken und die Risiken durch angemessene Maßnahmen auf ein tragbares Maß zu reduzieren. Grundlage dafür ist in Sachsen ab Sommer 2019 das Sächsische Informationssicherheitsgesetz (SächsISichG). Um in der IT der öffentlichen Verwaltung mit ihren ständigen technischen Weiterentwicklungen einen Zustand der Informationssicherheit zu gewährleisten, werden beständig personelle und finanzielle Ressourcen benötigt und zwar nicht nur in der IT selbst. Insbesondere organisatorische und auch bauliche Rahmenbedingungen müssen zielgerichtet mitgestaltet werden.

Informationssicherheit und deren Wahrnehmung ist nicht an einer bestimmten Stelle in einer Organisation angesiedelt. Da von jedem Computer, der Daten verarbeitet, potenziell die Informationssicherheit gefährdet werden kann, liegt die Verantwortung zur Gewährleistung der Informationssicherheit schlussendlich auch bei jeder Mitarbeiterin und jedem Mitarbeiter selbst. Insbesondere wenn personenbezogene Daten verarbeitet werden, geht es neben der Informationssicherheit auch um den Datenschutz. Diese beiden Kernaspekte gilt es bei der Planung, Einführung, Nutzung und der Aussonderung von IT stets zu berücksichtigen.

Die öffentliche Verwaltung des Freistaates Sachsen hat für ihren Bereich mit der Inkraftsetzung des Sächsischen E-Government-Gesetzes (SächsEGovG) im Jahr 2014 die Grundlagen für das eigene Handeln geschaffen und wird diese mit der geplanten Novellierung des SächsEGovG im Sommer 2019 an die sich ändernden Rahmenbedingungen anpassen. So bestimmt das Gesetz zum Beispiel das Serviceportal Amt24 als sächsisches Online-Verwaltungsportal im deutschlandweiten Portalverbund nach dem bundesweit gültigen Onlinezugangsgesetz (OZG) und verpflichtet die Verwaltung, den Bürgerinnen und Bürgern eine sichere elektronische Kommunikation anzubieten sowie Datenschutz- und Informationssicherheitskonzepte für die IT-Verfahren der Verwaltung zu erstellen.

Auch die Unternehmen in Sachsen sollen im Cyberraum sicher sein. Deswegen fördert der Freistaat den Ausbau des Informationsschutzes finanziell und arbeitet vor allem mit kleinen und mittleren Unternehmen in Projekten zur Erhöhung der Informationssicherheit zusammen, damit sächsisches Knowhow nicht in die Hände von Cyberkriminellen gerät. Für den Freistaat Sachsen von hoher strategischer Bedeutung ist daneben auch der Schutz der Betreiber kritischer Infrastrukturen (KRITIS), zum Beispiel Wasserwerke oder Krankenhäuser. Da die IT für die Daseinsvorsorge eine hohe Bedeutung hat, müssen geeignete Rahmenbedingungen und Maßnahmen zur übergreifenden Förderung der Informationssicherheit abgestimmt, etabliert und kontinuierlich weiterentwickelt werden. Grundlage dafür ist in erster Linie das IT-Sicherheitsgesetz des Bundes.

Schwerpunktbetrachtung: Informations- und Cybersicherheitseinrichtungen im Freistaat Sachsen

- Cybercrime Competence Center Sachsen (SN4C) des Landeskriminalamtes Sachsen mit der Zentralen Ansprechstelle Cybercrime (ZAC) für Unternehmen, Behörden und Verbände des Freistaates Sachsen
- Zentralstelle Cybercrime Sachsen (ZCS) der Generalstaatsanwaltschaft Dresden
- Lernlabore für IT-Sicherheit der Fraunhofer Gesellschaft an den Hochschulen Zittau/Görlitz sowie Mittweida zur Qualifikation von Fachleuten aus Wirtschaft und Behörden
- Beauftragter für Informationssicherheit des Landes (BfIS) als zentrale Instanz für die strategischen und koordinierenden Belange der Informationssicherheit in der Staatsverwaltung
- Computer Emergency Response Team für die Landesverwaltung Sachsen (SAX.CERT) beim Staatsbetrieb Sächsische Informatik Dienste (SID)

Operative Ziele[2]

- Den Schutz der IT-Systeme, Anwendungen und damit verbundener Datenbestände des Freistaates Sachsen ausbauen, zum Beispiel mit dem Projekt HoneySense
- Personalkapazitäten des Freistaates Sachsen im Bereich Informations- und Cybersicherheit sowie zur Bekämpfung von Cyberkriminalität verstärken
- Die Bevölkerung, Unternehmen und Angehörige der öffentlichen Verwaltung für Informations- und Cybersicherheit durch Informationsangebote und Veranstaltungen sensibilisieren, zum Beispiel mit der Roadshow „Die Hacker kommen“
- Kinder und Jugendliche in den Schulen zu Informations- und Cybersicherheit sensibilisieren
- Kleine und mittlere Unternehmen bei Maßnahmen zur IT Sicherheit unterstützen
- Jährlich mindestens 3.000 Angehörige von Behörden des Freistaates Sachsen im Bereich Informations- und Cybersicherheit fortbilden

2 Neben „Sachsen Digital“ trägt der Masterplan „Digitale Verwaltung Sachsen“ als weiterer strategischer Ansatz der Sächsischen Staatsregierung zur Erreichung der operativen Ziele bei.

2.1. Handlungsfeld: Sicherheit in der öffentlichen Verwaltung

Der Freistaat Sachsen will bei der Informations- und Cybersicherheit bezogen auf seine Verwaltungen als Vorbild für andere gesellschaftliche Bereiche vorangehen. Dazu gehört es unter anderem, die eigenen Mitarbeiterinnen und Mitarbeiter sowie Leitungsebenen ausreichend für das Thema zu sensibilisieren, bei der internen und externen Kommunikation sowie der Verarbeitung von Daten hohen Sicherheitsstandards zu entsprechen und geeignete Organisationsstrukturen aufzubauen sowie zu etablieren. Mit der Verwaltungsvorschrift zur Gewährleistung der Informationssicherheit in der Landesverwaltung (VwV IS) wurden bereits 2011 die Grundelemente für den Aufbau einer leistungsfähigen Organisation der Informationssicherheit in der Landesverwaltung geschaffen und sollen mit dem Sächsischen Informationssicherheitsgesetz (SächsISichG) im Sommer 2019 fortentwickelt werden:

1) der Beauftragte für Informationssicherheit des Landes (BfIS Land) als zentrale Sicherheitsinstanz,
2) die Arbeitsgruppe Informationssicherheit (AG IS) als Plattform der ressortübergreifenden Zusammenarbeit,
3) die Beauftragten für Informationssicherheit (BfIS) der Ressorts, der Polizei und des Staatsbetriebs Sächsische Informatik Dienste (SID) und
4) das Sicherheitsnotfallteam („Computer Emergency Response Team" – SAX.CERT) im SID.

Auf Basis dieser Organisationsstruktur werden die Vorgaben und Maßnahmen zur Informationssicherheit im Freistaat Sachsen abgestimmt und ausgebaut. Ziel ist es, die Informationssicherheit in den staatlichen und nichtstaatlichen Stellen im Freistaat Sachsen zu erhöhen und Gefahren für ihre informationstechnischen Systeme abzuwehren. Dafür sind kontinuierliche Anstrengungen notwendig, die beständig personelle und finanzielle Ressourcen binden.

2.2. Handlungsfeld: Sicherheit für Bürger und Unternehmen

Damit sowohl die Bürgerinnen und Bürger als private Nutzer von IT als auch Unternehmen die Potenziale der Digitalisierung vollständig ausschöpfen können, müssen sie besser als bislang über Risiken, Gefahren und Sicherheitsmaßnahmen informiert sein. Der zentrale Sicherheitsfaktor für die IT ist nicht eine technische Lösung, sondern der Mensch in seinem Umgang mit der Technik. Das Hauptaugenmerk des Freistaates liegt daher darauf, Wissensdefiziten und daraus resultierendem fahrlässigen Handeln entgegenzuwirken.

Die Landesverwaltung hat dabei je nach Zuständigkeitsbereich der jeweiligen Behörde die Möglichkeit, in einem geeigneten Rahmen bestimmte Zielgruppen aus der allgemeinen Öffentlichkeit mit spezifischen Maßnahmen für das Thema Cybersicherheit zu sensibilisieren. Informationsveranstaltungen, Schulungen und Fortbildungen für alle Altersgruppen der Bevölkerung sind im Sinne staatlichen Handelns unverzichtbar und unter anderem in den Bereichen Verbraucherschutz, schul- und ausbildungsergänzender Unterricht sowie berufsbegleitendes und lebenslanges Lernen denkbar.

Unternehmen sind grundsätzlich selbst für die Verbesserung der eigenen IT-Sicherheit verantwortlich. Jedoch stellt diese Aufgabe insbesondere für kleine und mittlere Unternehmen eine große Herausforderung dar. Der Freistaat Sachsen bietet ihnen daher bei entsprechenden Projekten Unterstützung an (Handlungsfeld 4.2). Im Bereich der kritischen Infrastrukturen (KRITIS) hat die IT-Sicherheit von Unternehmen, wie beispielsweise von Wasser- und Stromversorgern, neben der wirtschaftlichen auch eine hohe strategische Bedeutung für den Freistaat Sachsen. Hier setzen Maßnahmen direkt bei den Leitungsebenen der Unternehmen an und gehen weit darüber hinaus. So müssen zum Beispiel gemeinsame Strukturen für die Überwachung der IT-Sicherheit und für etwaige Notfallmaßnahmen geschaffen werden. Daher ist es das Ziel der Landesverwaltung, mit Institutionen und Einrichtungen, die zu den KRITIS gezählt werden, eng zusammenzuarbeiten.

2.3. Handlungsfeld: Bekämpfung der Cyberkriminalität

Die Angriffe auf die Integrität und Sicherheit von Datensystemen bergen ein sehr hohes Gefahrenpotenzial für die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft. Die Straftaten im Bereich der Cyberkriminalität werden weiter ansteigen und eine Vielzahl von Deliktbereichen umfassen. Die Cyberkriminalität nimmt dabei Ausmaße an, die weit über die amtlich registrierten Fälle hinausgehen. Nach Erkenntnissen des Landeskriminalamtes (LKA) wird im Bereich Cyberkriminalität nur ein geringer Anteil der Straftaten angezeigt. Dennoch steigt die Zahl der angezeigten Straftaten im Bereich Cyberkriminalität bislang immer weiter an.

Das Internet als Tatort bietet eine Vielzahl von Tatgelegenheiten, bleibt auf Dauer nur begrenzt kontrollierbar und kennt keine Staats- und Verwaltungsgrenzen. Cyberkriminelle nutzen stets die neuen technischen Entwicklungen, unterlaufen permanent technische Sicherheitsvorkehrungen und erschweren so Ermittlungen und Beweissicherungen. Die Täter bleiben zudem regelmäßig anonym, agieren schnell und oft arbeitsteilig. Dennoch muss das Strafverfolgungsmonopol des Staates durchsetzbar bleiben. Die mit der Digitalisierung einhergehende Verlagerung der Kriminalität ins Internet muss durch geeignete Verfolgungsmaßnahmen von staatlicher Seite aus bekämpft werden.

Aufgrund des rasanten technologischen Wandels bindet die Bekämpfung der Cyberkriminalität zunehmend Fortbildungsressourcen. Methoden der Ermittlungs- und Beweisführung müssen dem technologischen Fortschritt entsprechen und sind kostenintensiv. Nationale und internationale polizeiliche Zusammenarbeit sowie die Kooperation mit Wirtschaft, Forschung und Wissenschaft sind zu intensivieren.