ZIELBILD FÜR DAS SCHWERPUNKTTHEMA:

INFORMATIONSSICHERHEIT

„Verwaltungsmodernisierung. Mit Sicherheit." – Die öffentliche **Verwaltung im Dienst von Bürgerinnen und Bürgern sowie Unternehmen** nutzt zur Aufgabenerfüllung **sichere und resiliente Informationstechnik**. Der Einsatz **moderner und bedarfsgerechter Sicherheitstechnologien** gewährleistet die **Kontinuität der Verwaltungsverfahren** auf allen staatlichen Ebenen. Dabei wird die Skalierbarkeit der Lösungen an unterschiedlichen Rahmenbedingungen sichergestellt. Die dabei verarbeiteten **Daten** sind jederzeit angemessen **geschützt**. Die Verwaltung orientiert sich an folgenden **Leitprinzipien/Handlungsfeldern:**

Automatisierte Sicherheit

- Die in der Verwaltung eingesetzte Informationstechnik ist durch (teil-/voll-) automatisierte Prozesse der Erkennung, Bewertung und Beseitigung von Bedrohungen gekennzeichnet.
- Der Einsatz von aufeinander abgestimmten Schutzmechanismen und -prozessen führt zu einer auf die jeweilige Bedrohungslage angepassten Sicherheitsorchestrierung (SECaaS)*, die sich flexibel in unterschiedliche Verwaltungs- und IT-Strukturen integrieren lässt.
- In der gesamten IT-Infrastruktur ist das Modell der automatisierten und adaptiven Sicherheit implementiert.

Innovationsorientierte Sicherheit

- Sichere IT-Verfahren werden auf der Basis technologischer Entwicklungen laufend modernisiert.
- Zero Trust Architekturen bilden eine Grundlage der Informationssicherheit in der Verwaltung. Die Umsetzung berücksichtigt unterschiedliche bestehende IT-Strukturen und ermöglicht flexible, anpassbare Lösungen.
- Kritische IT-Verfahren werden durch eine quantensichere Verschlüsselung geschützt. Dabei werden übergreifende Strategien entwickelt, um eine möglichst breite und effiziente Implementierung sicherzustellen.

Risikobasierte Sicherheit

- In der Verwaltung ist ein wirksames Risikomanagement implementiert, auf dessen Grundlage Behördenleitungen angemessene (Investitions-)Entscheidungen treffen können.
- Die in der Verwaltung eingesetzte Soft- und Hardware wird nach dem Grundsatz ‚security by design' entwickelt. Sicherheitstests sind kontinuierlich in den Betriebsablauf integriert und an unterschiedliche Kapazitäten und Anforderungen angepasst.

Krisenresiliente Sicherheit

- Prozesse der IT-Notfallprävention und der IT-Notfallbewältigung sichern die Resilienz, Robustheit und Ausfallsicherheit bzw. Wiederherstellung kritischer IT-Verfahren („Continuity of Government").
- Angepasste IT-Notfalltrainings sind als Standardmaßnahme auf allen staatlichen Ebenen implementiert und gewährleisten eine praxisnahe Umsetzung in unterschiedlich strukturierten Organisationen.

Leadership in Sicherheit

- Experimentierräume für Informationssicherheit in der Verwaltung tragen dazu bei, neue Technologien, Verfahren und Methoden zu entwickeln, zu testen und effizient in verschiedenen Verwaltungsumgebungen einzuführen.
- In Experimentierräumen werden Interdisziplinarität und eine positive Fehlerkultur gelebt.
- Fachkräfte für Informationssicherheit werden gezielt zu Innovatoren und Designern für Informationssicherheit weiterentwickelt.

** Security as a Service*