Stärkung der Informationssicherheit durch ein effektives ISMS

Veröffentlicht am 27. Mai 2025

Ihre Ansprechpersonen: René Schwab, Jana Papritz

Tags: Erfolgsgeschichten, Öffentliche Verwaltung, Prozessoptimierung und -management

Das auftraggebende Bundesamt verarbeitet grosse Mengen an Daten, darunter zahlreiche besonders schützenswerte Personendaten sowie sensible Informationen. Um diese angemessen zu schützen, hat es uns mit der Einführung und Weiterentwicklung eines effektiven Informationssicherheits-Managementsystems (ISMS) beauftragt.

Um die Informationswerte wirksam zu schützen und die gesetzlichen Vorgaben aus dem Informationssicherheitsgesetz (ISG) und der zugehörigen Verordnung (ISV) nachweislich und vollumfänglich zu erfüllen, wurde das bestehende Informationssicherheits-Managementsystems (ISMS) gezielt ausgebaut und weiterentwickelt. Die grundlegenden Strukturen wurden überprüft, ergänzt und klarer definiert, um die Informationssicherheit wirksam zu steuern und nachhaltig im Betrieb zu verankern. Erfahren Sie, wie wir zur erfolgreichen Umsetzung des ISMS beigetragen haben.

Unser Vorgehen

Zu Beginn wurde eine strukturierte Auslegeordnung vorgenommen. Diese orientierte sich an den Kapiteln der ISO/IEC 27001-Norm und diente als Grundlage für die systematische Erhebung der bestehenden Strukturen und Prozesse. Gemeinsam mit den Auftraggebern wurde anschliessend das Zielbild für das ISMS erarbeitet. Dieses wurde danach mit der Ausgangslage abgeglichen, um das Vorgehen und den Handlungsbedarf zu bestimmen. Die erfassten Handlungsfelder wurden systematisch nach ihrer Relevanz für die Einhaltung der gesetzlichen Anforderungen und ihrem konkreten Beitrag zur Verbesserung der Informationssicherheit erfasst und priorisiert.

Die Umsetzung erfolgte in enger Abstimmung mit der Sicherheitsorganisation, dem Risikomanagement, dem Datenschutz sowie der obersten Führungsebene. Wir unterstützten den Auftraggeber nicht nur bei

konzeptionellen Fragen, sondern arbeiteten auch bei der Umsetzung und dem initialen Betrieb aktiv mit. Dabei haben wir insbesondere Aufgaben übernommen, die zur Entlastung der Informationssicherheitsbeauftragten Organisation (ISBO) beitrugen – etwa die Ausarbeitung von Richtlinien, die Pflege vom Schutzobjekt-Inventar, die Koordination zwischen den Beteiligten sowie die Integration sicherheitsrelevanter Aspekte ins Tagesgeschäft. Ein agiles, iteratives Vorgehen ermöglichte es, neue Prozesse schrittweise in den Betrieb zu integrieren, ihre Wirkung frühzeitig zu prüfen und bei Bedarf anzupassen. Die enge Verknüpfung mit dem operativen Alltag trug wesentlich zur Akzeptanz und Wirksamkeit der Massnahmen bei.

Ein zentrales Element der Arbeiten war der Aufbau eines einheitlich strukturierten und vollständig dokumentierten Schutzobjekt-Inventars. Für jedes Schutzobjekt wurde die Einstufung von Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit festgehalten. Ergänzend dazu wurde jedes Schutzobjekt anhand definierter Kriterien bewertet und einer Kritikalitätsstufe zugeordnet. In einem weiteren Schritt wurden die verantwortlichen Rollen definiert und die Schutzobjekte mit den zugehörigen Informationsobjekten, den bestehenden Risiken, allfälligen Ausnahmen sowie den an der Leistungserbringung beteiligten Lieferanten verknüpft. Das Schutzobjekt-Inventar ist heute die zentrale Referenz im ISMS. Viele weitere Elemente wie das Risikomanagement oder das Lieferantenmanagement stützen sich darauf. Es schafft Transparenz und ermöglicht eine gezielte, risikobasierte Steuerung der Informationssicherheit.

Zentrale Ergebnisse im Projektverlauf:

- Definieren von Anwendungsbereich und Verantwortlichkeiten, insbesondere bei Subventionen und Abgeltungen.
- Erstellung und Einführung der Erklärung zur Anwendbarkeit (SoA).
- Regelung der Rollen, Aufgaben und Zuständigkeiten im ISMS-Organisationshandbuch.
- Überarbeitung der ISMS-Richtlinien und -Konzepte gemäss ISO/IEC 27001 und Anpassung an ISG/ISV.
- Strukturierter Aufbau des Schutzobjekt-Inventars sowie dessen Verifizierung und Ergänzung mit den Verantwortlichen.
- Zuordnung der Lieferanten zu den Schutzobjekten und Bewertung ihrer Rolle in der Leistungserbringung.
- Einführung eines Risikomanagements inkl. Register, Behandlungsplan und Ausnahmenmanagement.
- Weiterentwicklung des Vorfallsmanagements und Integration in den operativen Betrieb.
- Aktive Pflege und Aktualisierung des Rechtsgrundlagenverzeichnisses.

- Umsetzung von Kommunikations- und Sensibilisierungsmassnahmen.

Das Schlussergebnis

Das Bundesamt verfügt heute über ein gut dokumentiertes, im Betrieb etabliertes und wirksam gelebtes ISMS. Die Rollen und Zuständigkeiten sind definiert, die relevanten Prozesse verankert, und ein kontinuierlicher Verbesserungsprozess ist in der Organisation etabliert. Das Schutzobjekt-Inventar schafft Transparenz über die Informationswerte, deren Schutzbedarf und die damit verbundenen Risiken. Die dadurch geschaffene Transparenz erlaubt eine gezielte Überwachung kritischer Elemente und die kontinuierliche Behebung identifizierter Schwächen.

Unsere Lessons Learned

Die Umsetzung hat gezeigt, dass der gezielte Ausbau bestehender Strukturen wirksamer war als eine komplette Neuerarbeitung. Obwohl die gesetzlichen Vorgaben den Anstoss gaben, steht heute die tatsächliche Verbesserung der Informationssicherheit im Vordergrund. Der frühzeitige Einbezug relevanter Stellen ermöglichte eine nahtlose Integration in die Organisation und eine rasche Umsetzung. Durch unsere aktive Mitarbeit konnte die Betriebsorganisation zudem operativ entlastet werden, was eine fokussierte Weiterentwicklung des ISMS erleichterte. Wesentlich ist auch die Erkenntnis, dass Informationssicherheit eine fortlaufende Aufgabe ist, die das aktive Mitwirken aller erfordert – im Sinne eines wirksamen und risikobasierten Managementsystems.

Fazit

Die erfolgreiche Umsetzung unterstreicht unsere Kompetenz in der Entwicklung und Umsetzung von ISMS-Lösungen. Mit fundierter Methodik, hohem Praxisbezug, pragmatischem Vorgehen und klarem Fokus auf Wirksamkeit haben wir einen nachhaltigen Beitrag zur Informationssicherheit beim Auftraggeber geleistet.

Möchten Sie erfahren, wie Informationssicherheit gezielt und wirksam gestärkt werden kann? Oder haben Sie andere Fragen zur Informationssicherheit in Ihrer Organisation? Wir unterstützen Sie gerne! Zögern Sie nicht uns per Telefon unter 058 320 30 00, per E-Mail unter office@app.ch oder mittels des untenstehenden Formulars zu kontaktieren. Unsere Expertinnen und Experten freuen sich auf Ihre Anfrage.