Cybersicherheit

Meldung von Vorfällen

Das Befolgen unterschiedlicher Vorgaben für Cyber-Security und Informationssicherheitsvorfälle macht das Leben der Pensionskassen nicht einfacher. Was sind die bestehenden Anforderungen, und was hält die Zukunft bereit?

Autoren: **Dominique Meier und Anja Aellen**

Der Gesetzgeber hat die Bedeutung der Informationssicherheit erkannt und in vielen Bereichen entsprechende Regelungen erlassen, die auch Pensionskassen betreffen. Derzeit ist der Geltungsbereich des W-ISDS auf die Durchführungsstellen der 1. Säule/Familienzulagen (FZ) beschränkt. In der 1. Säule werden diese Weisungen auch angewandt (siehe Kasten).

Meldepflicht gilt erst in der 1. Säule

Die aktuelle Herausforderung für Sozialversicherungen besteht darin, die umfassenden und teilweise nicht einheitlichen Vorgaben im Bereich der Informationssicherheit zu erfüllen.[1] Die Vorgaben der verschiedenen Regularien stimmen nicht immer überein, so dass für Pensionskassen einige offene Fragen bleiben. Im Hinblick auf die Meldepflichten kann die Praxis der 1. Säule nicht eins zu eins auf die 2. Säule übertragen werden.

Besonders deutlich wird dies am Beispiel der einzuhaltenden Meldepflichten bei einem Sicherheitsvorfall. Die unterschiedlichen Regelwerke stellen spezifische Vorgaben, die sorgfältig navigiert werden müssen, um zum einen Compliance sicherzustellen, zum anderen aber auch die Sicherheit der Daten zu gewährleisten.

Informationssicherheitsgesetz

Das Informationssicherheitsgesetz (ISG) mit seinen vier Ausführungsverordnungen trat am 1. Januar 2024 in Kraft. Die Revision des ISG ist beschlossen und soll voraussichtlich per 1. Januar 2025 in Kraft treten. Dieses umfasst eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen an das NCSC innerhalb von 24 Stunden nach deren Entdeckung. Zur Umsetzung der Neuerung wird zurzeit an einer Änderung der Ausführungsbestimmungen gearbeitet. Laut Art. 74b ISG sind nach Punkt i) davon auch Organisationen betroffen, die «Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen».

Datenschutzgesetz

Das Datenschutzgesetz (DSG) sieht eine Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vor, wenn eine Verletzung der Datensicherheit zu einem hohen Risiko für die betroffenen Personen führt. Je umfangreicher oder sensitiver die Datenbearbeitung bzw. der Datenbestand ist, desto eher ist ein hohes Risiko anzunehmen. Das hohe Risiko wird im Hinblick auf die Einwirkung auf die Identität, Selbstbestimmung oder

[1] Allgemein spricht man von einem Informationssicherheits-Management-System (ISMS). Dieses ist im Schema auf Seite 53 dargestellt.

Nützliche Links

Meldepflichten

Meldung an NCSC (BACS): bit.ly/Meldepflicht_NCSC

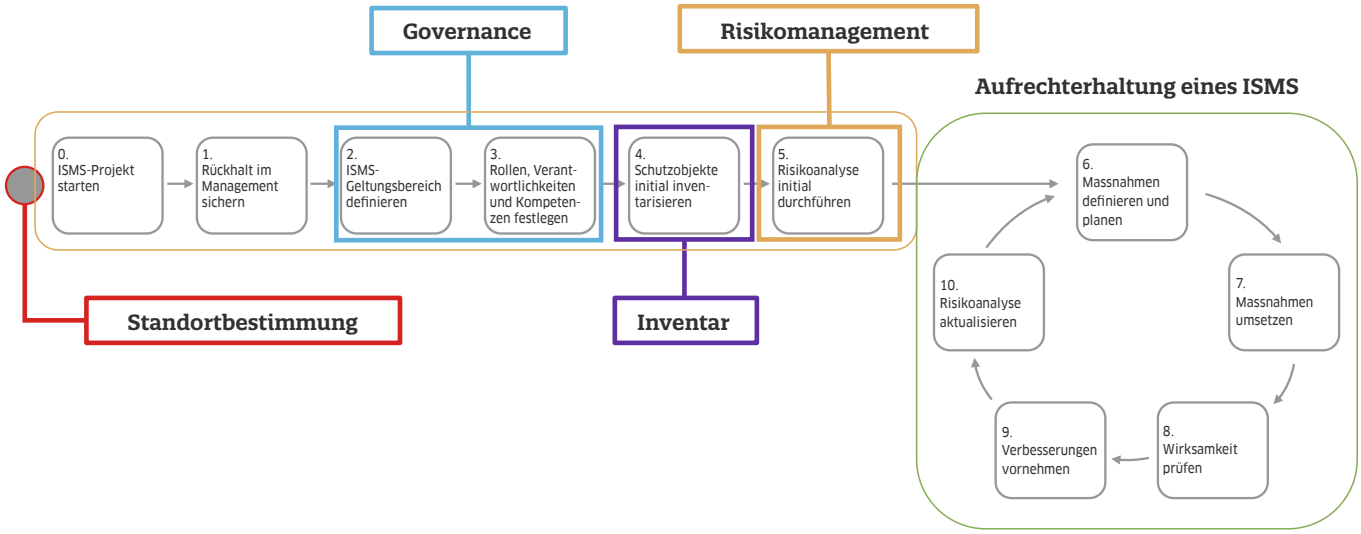
Meldung an Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB): bit.ly/Datenschutzportal

Meldung an Polizei: bit.ly/SwissCyberPolice

Checklisten

Verschiedene Anbieter bieten Checklisten zur Vorbereitung und zur Bewältigung eines Cybervorfalls zum Download an.

Aufbau und Aufrechterhaltung eines ISMS



Quelle: Redguard

Würde der betroffenen Person bestimmt. Eine Verletzung der Datensicherheit liegt u. a. vor, wenn Unbefugte durch einen Hackerangriff Datenzugriff erhalten. Dem EDÖB ist so schnell wie möglich nach Bekanntwerden des Vorfalls eine Meldung zu erstatten. Zudem sind die betroffenen Personen zu informieren, wenn dies zu deren Schutz erforderlich ist (z. B. bei gestohlenen Passwörtern) oder es durch den EDÖB verlangt wird.

Mit Pragmatik und Struktur Klarheit schaffen

Mit Blick auf die verschiedenen Regelwerke ist es empfehlenswert, einen strukturierten Ablauf zu definieren, der die Entscheidungsgrundlage bildet, wie mit den verschiedenen Anforderungen umzugehen ist. Dieser Ablauf umfasst das Verständnis und die Auflistung der verschiedenen Anforderungen, die Durchführung einer Risikobewertung zur Priorisierung der vorhandenen Ressourcen, die Definition von klaren Verantwortlichkeiten, die Festlegung von klaren Prozessen, z. B. Meldeprozessen, sowie die Schulung der eigenen Mitarbeitenden hinsichtlich der vorhandenen Pflichten und definierten Prozesse.

Um sicherzustellen, dass die relevanten Anforderungen ordnungsgemäss eingehalten werden und die definierten Prozesse kontinuierlich verbessert werden können, bedarf es zudem einer regelmässigen Überwachung sowie interner Compliance-Checks.

Die vorgenannten Elemente können mithilfe eines Informationssicherheits-Management-Systems (ISMS) strukturiert und pragmatisch aufgebaut werden. Ein ISMS bietet ein systematisches Vorgehen, heikle Informationen zu schützen, und wird unter anderem vom ISG, aber auch von den W-ISDS vorgeschrieben. Die Abbildung kann dabei helfen, dieses umfassende Vorhaben in einer strukturierten Weise zu starten und umzusetzen.

TAKE AWAYS

- Cybersecurity-Vorfälle müssen nicht nur gemeldet, sondern auch bewältigt werden.
- Zur Vorbereitung und Bewältigung eines Cybervorfalls gibt es bewährte Checklisten und Abläufe.

Anja Aellen

Security Consultant, Redguard AG

Dominique Meier

Partner, Head of Customer Success, Redguard AG

W-ISDS für die 1. Säule

Die Weisungen über die Anforderungen an die Informationssicherheit und den Datenschutz der Informationssysteme der Durchführungsstellen 1. Säule/FZ (W-ISDS) sind seit dem 1. Januar 2024 in Kraft. Sie gelten zurzeit nur für Organisationen der 1. Säule. Das W-ISDS fordert Meldungen an das BSV oder die jeweils zuständige Aufsichtsbehörde. Eine spezifische Frist wird nicht festgelegt.