Cybersécurité

Signalement des incidents

Suivre des directives différentes en matière de cybersécurité et d'incidents liés à la sécurité de l'information ne facilite pas la vie des caisses de pensions. Quelles sont les exigences actuelles et que nous réserve l'avenir?

Auteurs: **Dominique Meier et Anja Aellen**

Le législateur a reconnu l'importance de la sécurité de l'information et a édicté des réglementations correspondantes dans de nombreux domaines qui concernent également les caisses de pensions. Actuellement, le champ d'application des D-SIPD est limité aux organes d'exécution du 1er pilier/allocations familiales (AF). Ces directives sont effectivement appliquées dans le 1er pilier (voir encadré).

L'obligation de déclarer ne s'applique qu'au 1er pilier

Le défi actuel pour les assurances sociales consiste à se conformer aux directives complètes et parfois non uniformes dans le domaine de la sécurité de l'information.[1] Les prescriptions des différentes réglementations ne concordent pas toujours, de sorte que certaines questions restent ouvertes pour les caisses de pensions. En ce qui concerne les obligations de déclaration, la pratique du 1er pilier ne peut pas être transposée une à une au 2e pilier.

L'exemple des obligations de notification à respecter en cas d'incident de sécurité le montre bien. Les différents cadres réglementaires imposent des contraintes spécifiques qu'il convient de naviguer avec soin afin de garantir d'une part la conformité, mais aussi la sécurité des données.

Loi sur la sécurité de l'information

La loi sur la sécurité de l'information (LSI) et ses quatre ordonnances d'exécution sont entrées en vigueur le 1er janvier 2024. La révision de la LSI a été décidée et devrait entrer en vigueur le 1er janvier 2025. Celle-ci comprend une obligation de notification des cyberattaques contre les infrastructures critiques au NCSC dans les 24 heures suivant leur découverte. Pour mettre en œuvre cette nouveauté, une modification des dispositions d'exécution est en cours. Selon l'art. 74b LSI, point i), sont également concernées les organisations qui «fournissent des prestations de couverture contre les conséquences de la maladie, de l'accident, de l'incapacité de travail et de gain, de la vieillesse, de l'invalidité et de l'impotence».

Loi sur la protection des données

La loi sur la protection des données (LPD) prévoit une obligation de notification au Préposé fédéral à la protection des données et à la transparence (PFPDT) lorsqu'une violation de la sécurité des données entraîne un risque élevé pour les personnes concernées. Plus le traitement des données ou le stock de données est important ou sensible, plus il est probable que le risque soit élevé. Le risque élevé

[1] On parle généralement d'un système de gestion de la sécurité de l'information (SGSI). Celui-ci est représenté dans le schéma de la page 53.

Liens utiles

Obligations de déclaration

Déclaration au NCSC (OFCS): bit.ly/Meldepflicht_NCSC

Annonce au Préposé fédéral à la protection des données et à la transparence (PFPDT): bit.ly/Portail sur la protection des données

Déclaration à la police: bit.ly/SwissCyberPolice

Listes de contrôle

Plusieurs fournisseurs proposent des listes de contrôle à télécharger pour se préparer et gérer un cyber incident.

est déterminé par rapport à l'impact sur l'identité, l'autodétermination ou la dignité de la personne concernée. Il y a notamment violation de la sécurité des données lorsque des personnes non autorisées ont accès aux données suite à un piratage. Une déclaration doit être faite au PFPDT le plus rapidement possible après avoir pris connaissance de l'incident. En outre, les personnes concernées doivent être informées si cela est nécessaire pour leur protection (p. ex. en cas de vol de mots de passe) ou si le PFPDT l'exige.

Créer de la clarté avec pragmatisme et structure

Compte tenu des différents cadres réglementaires, il est recommandé de définir un processus structuré qui servira de base de décision quant à la manière de traiter les différentes exigences. Ce processus comprend la compréhension et l'énumération des différentes exigences, la réalisation d'une évaluation des risques afin de prioriser les ressources disponibles, la définition de responsabilités claires, la définition de processus clairs, par exemple les processus de notification, ainsi que la formation des propres collaborateurs en ce qui concerne les obligations existantes et les processus définis.

Pour s'assurer que les exigences pertinentes sont dûment respectées et que les processus définis peuvent être continuellement améliorés, il faut en outre une surveillance régulière ainsi que des contrôles de conformité internes.

Les éléments susmentionnés peuvent être mis en place de manière structurée et pragmatique à l'aide d'un système de gestion de la sécurité de l'information (SGSI). Un SGSI offre une approche systématique de la protection des informations sensibles et est notamment prescrit par la LSI, mais aussi par les D-SIPD. Le schéma peut aider à lancer et à mettre en œuvre ce vaste projet de manière structurée.

TAKE AWAYS

- Les incidents de cybersécurité ne doivent pas seulement être signalés, ils doivent aussi être gérés.
- Il existe des listes de contrôle et des procédures éprouvées pour se préparer et gérer un cyber incident.

D-SIPD pour le 1er pilier

Les directives relatives aux exigences en matière de sécurité de l'information et de protection des données des systèmes d'information des organes d'exécution du 1er pilier/AF (D-SIPD) sont en vigueur depuis le 1er janvier 2024. Elles ne s'appliquent actuellement qu'aux organisations du 1er pilier. Les D-SIPD exigent des déclarations à l'OFAS ou à l'autorité de surveillance compétente respective. Aucun délai spécifique n'est fixé.