APP Unternehmensberatung AG

Guide pratique :
Sécurité de l’information pour les cadres



La sécurité de l’information constitue une responsabilité partagée par l’ensemble de l’organisation. Toutefois, sa gestion stratégique, sa planification tactique et sa mise en œuvre opérationnelle relèvent de la responsabilité des cadres. Cela nécessite des principes clairs, des processus harmonisés et une compréhension commune, afin de garantir que les organisations demeurent sûres et pleinement opérationnelle.

Nous présentons ci-après des recommandations concrètes en matière de sécurité de l’information à l’intention des cadres, et illustre la manière dont celles-ci peuvent être intégrées efficacement aux niveaux stratégique, tactique et opérationnel.



Niveau stratégique

Le niveau stratégique met l'accent sur les aspects à long terme et directeurs de la sécurité de l'information, car sans ces décisions fondamentales, les niveaux inférieurs risquent également d'échouer.



Principes directeurs et culture

Adoptez les principes directeurs de la sécurité de l'information et intégrez-les durablement dans la culture de votre organisation.

Exemples

- Intégrez le Security by Design en prenant en compte les aspects de sécurité dès le début du développement des produits et des services.
- Encouragez une culture d'apprentissage et de signalement ouverte.



Stratégie et conditions-cadres

Intégrez la sécurité de l'information dans la stratégie à long terme de votre organisation et définissez un cadre clair pour la gestion des partenaires, des risques et des ressources.

Exemples

- Gérez vos partenariats de manière stratégique, tant sur le plan technologique (cloud vs. sur site) que sur le plan organisationnel (standardisation vs. innovation).
- Établissez des exigences précises pour vos partenaires et définissez les critères, normes et preuves attendues régulièrement (p. ex. preuve de conformité à la norme ISO 27001).
- Assurez une gestion rigoureuse des informations sensibles et des données personnelles. Une perte de données peut entraîner des dommages importants à la réputation et doit donc être considérée comme un risque stratégique.



Décisions d'investissement

Prenez des décisions d'investissement fondamentales concernant les technologies et les ressources nécessaire à acquérir.

Exemples

- Lorsque des informations sensibles et des données personnelles doivent être traitées, choisissez un partenaire disposant d'un centre de données en Suisse.
- Évaluez l'opportunité de créer et d'exploiter un « Security Operations Center » en interne ou d'en confier la gestion à un prestataire externe (make or buy).



Objets et objectifs de protection

Déterminez les principaux objets de protection (ressources informationnelles, qu'ils soient ou non fondés sur des systèmes informatiques) et définissez les objectifs de protection au sein de la chaîne de valeur.

Exemple

- Définissez comme objets de protection les ensembles d'informations liés aux données clients ou à la propriété intellectuelle, et fixez les objectifs de protection CIA (Confidentiality (C), Integrity (I), Availability (A)).

Niveau tactique

Le niveau tactique traduit les orientations stratégiques en structures et processus concrets au sein de l'organisation, veillant à ce que la sécurité de l'information soit non seulement planifiée, mais aussi mise en œuvre.

Conception des achats et fournisseurs

Intégrez la sécurité de l'information dès le départ dans la conception des achats et tout au long de la gestion des fournisseurs.

Exemples

- Intégrez des rôles spécialisés en sécurité de l'information (ISBO, CISO) dans votre équipe d'achats.
- Adoptez les directives stratégiques et complétez-les par des exigences spécifiques à la sécurité de l'information dans les processus d'approvisionnement, notamment en intégrant dans les contrats des clauses liées aux certifications ou aux mesures de sécurité.

Responsabilités et autorisations

Alignez les responsabilités sur les directives et les bases légales existantes, et mettez-les en œuvre de manière ciblée dans les concepts d'autorisation conformément au principe du besoin de savoir (need to know).

Exemples

- Désignez dès le lancement d'un projet les responsables des objets de protection et les propriétaires des risques, tant pour la phase de réalisation que pour son exploitation ultérieure.
- Tenez compte du principe de la double validation lors de l'attribution des droits d'accès aux informations sensibles.
- Prévoyez consciencieusement des vérifications périodiques, telles que la révision des droits d'accès, afin d'éviter que d'anciens collaborateurs, partenaires ou comptes de test spéciaux conservent un accès prolongé à vos systèmes.

Compétences, lacunes et formation continue

Assurez-vous que les compétences adéquates sont présentes, que les éventuelles lacunes soient identifiées à temps et que les ressources nécessaires – notamment le temps et les moyens financiers – soient allouées à la formation continue.

Exemples

- Proposez des formations adaptées aux rôles et aux niveaux. Les collaborateurs ont besoin d'une mise à jour régulière sur le thème du « comportement dans la gestion des informations ». Les propriétaires de risques doivent être formés sur des sujets tels que « situation actuelle des menaces » ou « évaluation et traitement des risques ».
- Évaluez individuellement les compétences (matrice de compétences) et actualisez les contenus de formation en fonction des derniers développements.

Collaboration interdisciplinaire

Coordonnez la collaboration interdisciplinaire lors de la mise en œuvre de la stratégie de sécurité de l'information.

Exemples

- Organisez régulièrement des réunions et des analyses d'interfaces entre l'informatique, la sécurité de l'information et les domaines métiers afin de renforcer la collaboration interdisciplinaire au sein des équipes.
- Encouragez la création de Communities of Practice (par exemple en réunissant les responsables de projets de protection afin d'échanger sur les approches et les problématiques actuelles).

Niveau opérationnel

Le niveau opérationnel comprend la mise en œuvre quotidienne des mesures de sécurité de l'information et leur amélioration continue.

Communication et exemplarité

Intégrez la culture de la sécurité dans vos pratiques quotidiennes, et favorisez une communication transparente au sein de l'équipe.

Exemples

- En tant que cadre, donnez l'exemple en parlant ouvertement des risques de sécurité avec votre équipe.
- Instaurer une culture ouverte de l'erreur en discutant régulièrement et de manière transparente des lessons learned.

Capacité d'action et amélioration

Assurez en permanence la capacité d'action et visez une amélioration continue.

Exemples

- Définissez et formez des remplaçants pour tous les rôles liés à la sécurité.
- Dérivez des mesures concrètes à partir des lessons learned et mettez-les en œuvre rapidement. Par exemple, demandez des ressources humaines supplémentaires, si vous constatez que le dispositif de remplacement ne peut pas être appliqué de manière cohérente.

Gestion et réduction des risques

Gérez en continu les risques associés aux objets à protéger et déployez les mesures adaptées pour les réduire.

Exemples

- Donnez la priorité à la mise en place d'une authentification multifacteur avant toute mise à jour esthétique de l'interface utilisateur.
- Vérifiez régulièrement, en particulier lors de modifications liées à la sécurité, que le niveau de protection de vos actifs reste adéquat. Ajustez-le si nécessaire, notamment lorsque vous traitez de nouvelles données personnelles sensibles.

Changements de l'environnement

Surveillez de manière proactive les changements externes dans votre environnement (notamment celui des fournisseurs).

Exemples

- Mettez en place un dispositif de surveillance pour suivre les évolutions législatives, les tendances technologiques et les nouvelles menaces. Analysez leur impact et définissez les mesures appropriées.
- Assurez-vous de bien connaître la chaîne d'approvisionnement de vos objets à protéger et anticipez les changements. Par exemple, le rachat d'un fournisseur par un grand groupe peut entraîner des modifications des conditions contractuelles ou du respect des exigences de sécurité.

Nos expertes et experts

Nous serons ravis de vous accompagner dans l'intégration efficace de la sécurité de l'information au sein de votre organisation – de la définition de la stratégie à la mise en œuvre quotidien. N'hésitez pas à nous contacter pour découvrir comment nous pouvons vous soutenir dans cette démarche.

www.app.ch/infosec



Tél. +41 58 320 30 25
E-mail andreas.steiner@app.ch



Tél. +41 58 320 30 38
E-mail jana.papritz@app.ch