CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

PL-08

Architecture de sécurité et de protection de la vie privée

Juill. 2026

Votre gouvernement

Québec

PL

Planification de la cybersécurité

Planning

PL-08 — Architecture de sécurité et de protection de la vie privée (PaFF)

Énoncés :

a. Élaborer des architectures de sécurité et de protection de la vie privée pour le système qui décrit :
- **1.** les exigences et l'approche à adopter pour protéger la confidentialité, l'intégrité et la disponibilité de l'information de l'organisation
- **2.** les exigences et l'approche à adopter pour traiter les renseignements personnels de manière à limiter les risques d'atteinte à la vie privée des personnes
- **3.** la façon dont les architectures sont intégrées à l'architecture d'entreprise et prises en charge par cette dernière
- **4.** toutes les hypothèses en lien avec les services et systèmes externes et les interdépendances

b. Passer en revue et mettre à jour les architectures [Affectation : fréquence définie par l'organisation] de manière à tenir compte des changements apportés à l'architecture d'entreprise
c. Refléter les changements prévus à l'architecture dans les plans de sécurité et de protection de la vie privée, le CONOPS, l'analyse de criticité, les procédures organisationnelles, de même que l'approvisionnement et les acquisitions

Responsable : Aucun

Discussion :

Les architectures de sécurité et de protection de la vie privée au niveau du système sont conformes aux architectures de sécurité et de protection de la vie privée de l'organisation décrites dans le contrôle PM-
07. Elles en font partie intégrante et sont développées dans le cadre de l'architecture d'entreprise. Les architectures comprennent une description de l'architecture, l'affectation des fonctions de sécurité (dont les contrôles), l'information relative à la sécurité et à la protection de la vie privée des interfaces externes, l'information échangée entre les interfaces, le flux de données des renseignements personnels et les mécanismes de protection associés à chacune des interfaces. Les architectures peuvent également comprendre d'autres renseignements, comme les rôles des utilisateurs et les privilèges d'accès associés à chacun de ces rôles; les exigences propres à la sécurité et à la protection de la vie privée; les types de renseignements traités, stockés et transmis par les systèmes; les exigences relatives à la gestion des risques liés à la chaîne d'approvisionnement; les priorités de restauration de l'information et des services des systèmes, ainsi que tout autre besoin de protection. Il est important de respecter l'orientation pertinente sur l'utilisation des architectures de sécurité dans le cadre du processus du cycle de développement des systèmes. Le Centre pour la cybersécurité recommande d'adopter les concepts d'ingénierie de la sécurité des systèmes décrits dans le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037). Les architectures de sécurité et de protection de la vie privée sont examinées et mises à jour tout au long du cycle de développement des systèmes, de l'analyse des alternatives à l'examen de l'architecture proposée dans les propositions de marché et aux revues de conception réalisées avant et durant la mise en oeuvre (par exemple, durant les revues de conception préliminaires et de conception critiques). Dans les architectures informatiques modernes, de moins en moins d'organisations contrôlent l'ensemble des ressources d'information. Les organisations pourraient dépendre fortement des services d'information externes et des fournisseurs de services. Il est nécessaire de décrire ces dépendances dans l'architecture de sécurité et de protection de la vie privée pour mettre en place une stratégie de protection exhaustive de la mission et des activités. La mise en oeuvre et le maintien d'architectures efficaces passent essentiellement par l'élaboration, le développement, la documentation et le maintien d'une configuration de base pour les systèmes de l'organisation dans le cadre du contrôle des configurations. Le développement des architectures est coordonné avec le bureau de la ou du CSIO de l'organisme, la ou le haut fonctionnaire chargé de la gouvernance de sécurité du ministère, ainsi que la ou le cadre supérieur en matière de protection de la vie privée pour veiller à ce que les contrôles nécessaires pour soutenir les exigences propres à la sécurité et à la protection de la vie privée soient établies et mises en oeuvre efficacement. Dans plusieurs cas, il pourrait n'y avoir aucune distinction entre les architectures de sécurité et de protection de la vie privée d'un système. Dans d'autres cas, il est possible d'atteindre adéquatement les objectifs liés à la sécurité, alors que ceux liés à la protection de la vie privée ne sont que partiellement satisfaits par les exigences relatives à la sécurité. Dans de tels scénarios, le fait d'avoir à considérer l'imposition d'exigences en matière de protection de la vie privée pour atteindre les objectifs donnera lieu à la mise en oeuvre d'une architecture de protection de la vie privée distincte. La documentation pourrait toutefois ne faire mention que des architectures combinées. Le contrôle PL-08 concerne principalement les organisations. Il vise à s'assurer que ces dernières mettent en place des architectures pour le système, et que ces architectures s'intègrent à l'architecture d'entreprise ou y soient étroitement liées. Par opposition, le contrôle SA-17 concerne principalement les développeuses, les développeurs, les intégratrices et les intégrateurs de produits et de systèmes de TI externes. Les organisations sélectionnent le contrôle SA-17, qui est complémentaire au contrôle PL-08, lorsqu'elles externalisent le développement des systèmes ou des composants connexes à des entités externes et dans la mesure où il est nécessaire d'assurer l'uniformité avec l'architecture d'entreprise et les architectures de sécurité et de protection de la vie privée de l'organisation.