Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Guide sur la segmentation en unités dans le cadre des services fondés sur l'infonuagique

ITSP.50.108

SÉRIE PRATICIEN

TLP:WHITE

Canada

Avant-propos

L'ITSP.50.108, *Guide sur la segmentation en unités dans le cadre des services fondés sur l'infonuagique*, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

Ce guide fait partie d'une série de documents élaborés par le Centre pour la cybersécurité dans le but de sécuriser les services fondés sur l'infonuagique. Il appuie l'approche de gestion des risques liés à la sécurité infonuagique établie dans l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique* [1][1].

Pour obtenir de l'information supplémentaire ou proposer des modifications au présent document, prière de communiquer avec notre centre d'appel par courriel ou par téléphone :

Centre d'appel
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 6 octobre 2021.

Historique des révisions

Révision	Modifications	Date
1.	Première version.	6 octobre 2020

ISBN 978-0-660-40519-3
CAT D97-3/50-108-2021F-PDF

[1] Les numéros entre crochets renvoient à du matériel de référence figurant à la section Contenu complémentaire du présent document.

Vue d'ensemble

L'information fournie dans le présent document d'orientation sur la sécurité s'adresse aux organisations des secteurs privé et public. Votre organisation peut appliquer ces conseils à tous les services fondés sur l'infonuagique, quels que soient les modèles de déploiement en nuage et les services infonuagiques. Pour en savoir plus sur les services infonuagiques et les modèles de déploiement, consultez l'ITSAP.50.111, *Modèles de l'infonuagique* [2].

Table des matières

Liste des figures

1 Introduction

Le présent document décrit la façon dont votre organisation peut avoir recours à la segmentation en unités pour réduire le risque résiduel lié à l'utilisation des services fondés sur l'infonuagique pour la transmission, le traitement ou le stockage d'information sensible (c'est-à-dire l'information qui doit être protégée contre toute divulgation non autorisée). Lorsque votre organisation utilise des services infonuagiques, elle continue d'être légalement responsable de ses systèmes et de ses données. Il vous revient de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des systèmes d'information qui sont hébergés par un fournisseur de services infonuagiques (FSI).

Dans le cadre de son architecture de sécurité axée sur la défense en profondeur, votre organisation peut mettre en œuvre la segmentation en unités afin de protéger l'information sensible et de réduire les risques de compromission. La segmentation en unités consiste à générer une valeur de remplacement (appelée un jeton) et à substituer celle-ci à l'information ou aux données d'origine. Cette technique, employée à grande échelle dans les secteurs des finances et des soins de santé, est conçue de manière à protéger des champs de données discrètes dans les systèmes d'information.

1.1 Règlements et politiques applicables

Il est parfois difficile d'assurer la conformité aux politiques et aux règlements applicables lorsque vous avez recours à des services fondés sur l'infonuagique, car votre organisation et le FSI exercent tous deux un contrôle direct sur de nombreux aspects de la sécurité et du respect de la vie privée. Or, il revient à votre organisation de veiller à ce qu'elle respecte les exigences de l'ensemble des politiques et des règlements applicables, des lois provinciales et territoriales sur la protection de la vie privée et des règlements et des normes propres à votre secteur. Les politiques et les règlements comme la *Loi sur la protection des renseignements personnels* [3] et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) [4] régissent la manière dont les organisations canadiennes peuvent stocker, transmettre et traiter des renseignements personnels. Au sein des ministères et organismes du gouvernement du Canada (GC), des mentions de sécurité servent à désigner l'information sensible et à indiquer le niveau de préjudice lié à l'éventuelle compromission de l'information. Pour en savoir plus sur les exigences relatives à la protection de l'information sensible, veuillez consulter les ressources ci-dessous :

- Secrétariat du Conseil du Trésor du Canada, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la politique sur la sécurité [5];
- Commissariat à la protection de la vie privée du Canada, *L'infonuagique pour les petites et moyennes entreprises* [6].

Plusieurs politiques et normes portent sur la mise en œuvre de la segmentation en unités dans le but de sécuriser les paiements et d'autres transactions financières, notamment :

- Conseil des normes de sécurité PCI, *Payment Card Industry Data Security Standard (PCI DSS) Information Supplement: PCI DSS Tokenization Guidelines* [7];
- American National Standards Institute (ANSI), ASC/X9 – *ANSI X9.119-2 Requirements for Protection of Sensitive Payment Card Data – Part 2: Implementing Post-Authorization Tokenization Systems* [8].

Consultez ces ressources et d'autres politiques, normes et lignes directrices applicables pour prendre connaissance des recommandations sur la mise en œuvre de la segmentation en unités pour sécuriser les transactions de paiement.

1.2 Gestion des risques liés à l'infonuagique

En appliquant des pratiques de gestion des risques liés à la sécurité des TI, y compris des stratégies de défense en profondeur pour les services infonuagiques, votre organisation peut atténuer les risques associés à l'utilisation de services infonuagiques pour stocker, transmettre et traiter de l'information sensible. La publication ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [9] du Centre pour la cybersécurité définit deux niveaux d'activités de gestion des risques : les activités de gestion des risques au niveau organisationnel (ou ministériel) et celles associées aux systèmes d'information. Vous pouvez intégrer les activités associées au niveau organisationnel au programme de sécurité de votre organisation pour planifier, évaluer et améliorer la gestion des risques liés à la sécurité des TI. À ce niveau, la segmentation en unités appuie la gestion des risques organisationnels en définissant les approches de sécurité pour les profils de contrôle de sécurité de votre organisation. Le Centre pour la cybersécurité a établi des profils de contrôle de sécurité pour les services fondés sur l'infonuagique selon les profils de base présentés à l'annexe 4 de l'ITSG-33 [9].

Vous pouvez intégrer les activités au niveau des systèmes d'information au cycle de développement des systèmes (CDS) de votre organisation. Ces activités comprennent l'ingénierie de sécurité, l'évaluation des menaces et des risques, l'évaluation de la sécurité et l'autorisation des systèmes d'information. L'approche de gestion des risques liés à la sécurité infonuagique du Centre pour la cybersécurité s'aligne sur les activités au niveau des systèmes d'information. La mise en œuvre de la segmentation en unités s'inscrit dans l'étape cinq de l'approche de gestion des risques liés à la sécurité infonuagique. La segmentation en unités appuie également l'architecture de sécurité axée sur la défense en profondeur, qu'on peut appliquer à la conception et à la mise en œuvre de contrôles de sécurité infonuagiques.

1.3 La défense en profondeur pour les services fondés sur l'infonuagique

Comme l'indique l'ITSP.50.104, *Guide sur la défense en profondeur pour les services fondés sur l'infonuagique* [10], les technologies de segmentation en unités permettent de protéger l'information et les systèmes sensibles dans le cadre de la troisième couche de défense (sécurité des données). Votre organisation doit prendre en considération la manière dont l'information sensible sera protégée pendant sa transmission à destination, en provenance et à l'intérieur d'environnements infonuagiques. Vous devez également vous assurer que l'information sensible est protégée lorsqu'elle est au repos dans le nuage et lorsqu'elle est traitée dans tous les référentiels de réplication de données. De plus, vous devez veiller à ce que cette information soit protégée après la mise hors service des systèmes d'information connexes. La segmentation en unités constitue l'une des technologies qui vous permettront de répondre à ces exigences.

2 Segmentation en unités

La segmentation en unités consiste à générer une valeur de remplacement (un jeton) et à substituer celle-ci à l'information ou aux données d'origine. De nombreux systèmes de segmentation en unités permettent également de renverser le processus (désegmentation des unités), c'est-à-dire de remplacer le jeton par les données ou l'information d'origine.

Le jeton peut servir d'identifiant qui renvoie aux données d'origine. Les jetons générés correctement ne contiennent aucune information sensible et peuvent être transmis, stockés et traités à la place des données d'origine. Le risque résiduel lié à la confidentialité et à l'intégrité de l'information d'origine est réduit, car seuls les systèmes d'information, y compris le système de segmentation en unités, ont accès à l'information sensible d'origine.

La segmentation en unités ressemble au chiffrement dans le sens où les deux techniques peuvent être utilisées pour masquer l'information sensible. La segmentation en unités et le chiffrement comportent tous deux des avantages pour la protection de l'information, et ils sont souvent utilisés conjointement. Alors que le chiffrement a recours à des processus de codage réversibles et à des clés de chiffrement, les jetons, eux, ne sont pas liés aux données d'origine par une fonction mathématique (sauf dans le cas des systèmes de segmentation en unités qui utilisent des modèles de chiffrement réversibles pour générer des jetons). Le déchiffrement inverse le processus de chiffrement pour rétablir le texte chiffré en texte en clair. L'information d'origine représentée par un jeton est stockée et mappée dans la base de données de désegmentation des unités. Les systèmes de segmentation en unités comportent de nombreux avantages, notamment des méthodologies de segmentation en unités conçues de manière à vous permettre de traiter, de rechercher et de trier les données d'origine en n'utilisant que les jetons qui y sont associés.

2.1 Processus de segmentation en unités

Les solutions de segmentation en unités varient considérablement selon le fournisseur, les besoins opérationnels et l'architecture des systèmes d'information pris en charge. Dans le cadre du processus de gestion des risques liés à la sécurité infonuagique de votre organisation, vous devrez évaluer les modèles de déploiement disponibles, les méthodes de segmentation et de désegmentation, et les processus de segmentation en unités dans le but de déterminer la solution qui répond le mieux aux besoins de votre organisation.

2.1.1 Activités liées au processus de segmentation en unités

Nous décrivons ici un service de base de segmentation en unités qui pourrait aider à protéger l'information sensible dans un système qui utilise des services fondés sur l'infonuagique.

Dans un système fondé sur l'infonuagique, six activités principales utilisent la segmentation en unités afin de protéger l'information sensible (voir la figure 1).

1. L'information sensible est recueillie, générée ou récupérée à partir de sources de données existantes, puis elle est transmise au serveur de segmentation en unités.
2. Les applications du serveur de segmentation en unités reconnaissent les champs contenant de l'information sensible en fonction de règles et de stratégies définies au préalable et génèrent des jetons aléatoires ou semi-aléatoires pour ces champs. L'information d'origine, les jetons connexes et les données de mappage sont stockés dans la base de données de segmentation en unités.

3. Les jetons sont envoyés aux services fondés sur l'infonuagique de votre organisation, où ils sont stockés.
4. L'information segmentée en unités peut être intégrée à d'autres sources d'information et traitée, distribuée et stockée ailleurs, selon les besoins opérationnels de votre organisation.
5. Lorsque les applications et les utilisateurs autorisés en ont besoin, l'information agrégée ou traitée contenant l'information segmentée en unités est extraite des services infonuagiques.
6. Les applications et les utilisateurs autorisés envoient des requêtes au serveur de segmentation en unités, qui indiquent les jetons associés à l'information d'origine dont ils ont besoin. Le serveur de segmentation en unités renvoie les valeurs d'information d'origine aux applications et utilisateurs autorisés.

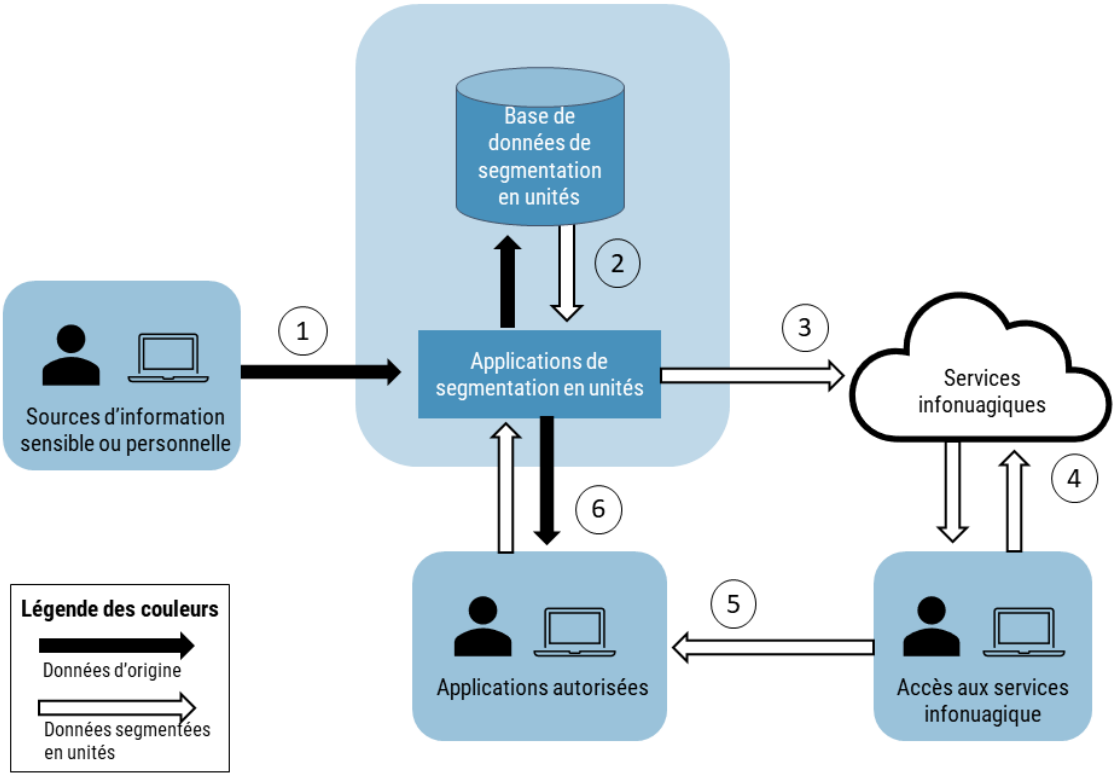

Figure 1 : **Service de base de segmentation en unités pour les services fondés sur l'infonuagique**

2.2 Modèles de génération de jetons

Il existe peu de normes internationales sur la segmentation en unités, sauf dans l'industrie des cartes de paiement. Les méthodes et les technologies utilisées pour produire, stocker et gérer les jetons varient considérablement d'un fournisseur à l'autre. En général, les systèmes de segmentation en unités conçus pour protéger l'information sensible génèrent des jetons qui correspondent au format des données d'origine. Il est ainsi plus facile de traiter, de rechercher et de trier les jetons. Les applications et les bases de données utilisent les jetons de format correspondant comme substituts directs des valeurs d'origine sans devoir adapter les applications.

Voici les trois modèles de génération de jetons courants :

- **Attribution aléatoire sur demande :** Un générateur de nombres aléatoires (RNG pour *Random Number Generator*) produit un nombre ou une séquence alphanumérique au hasard pour chaque champ ou valeur d'information.
- **Segmentation en unités statique basée sur une table :** Un RNG ou un générateur de nombres pseudo-aléatoires (PRNG pour *Pseudo-Random Number Generator*) est utilisé pour remplir une table à partir de laquelle les jetons sont sélectionnés par la suite.
- **Segmentation en unités basée sur le chiffrement :** Les jetons sont générés par des méthodes de chiffrement, notamment l'utilisation d'une clé symétrique avec des algorithmes de code d'authentification de message. Les modèles de segmentation en unités basée sur le chiffrement peuvent produire soit des jetons qu'il est possible de déchiffrer afin de rétablir les valeurs d'origine, soit des jetons unidirectionnels qu'il est impossible de déchiffrer. Les jetons générés par chiffrement pourraient également correspondre au format des valeurs d'origine si des algorithmes de chiffrement préservant le format (FPE pour *Format-Preserving Encryption*) sont utilisés.
  - Pour en savoir plus, consultez le document *Special Publication 800-38G Recommendation for Block Cypher Modes of Operation: Methods for Format-Preserving Encryption* [11] du National Institute of Standards and Technology (NIST).

Pour obtenir de l'information supplémentaire sur ces trois méthodes, veuillez consulter la norme ANSI X9 119-2 de l'ASC/X9 [8].

2.3 Serveurs de segmentation en unités

La plupart des systèmes de segmentation en unités reposent sur des serveurs de segmentation en unités. Ces serveurs créent et stockent les jetons, en plus de prendre en charge les fonctions de sécurité qui protègent l'information sensible qu'ils stockent, traitent et transmettent. Ces fonctions de sécurité comportent l'authentification des applications et des utilisateurs qui accèdent au serveur de segmentation en unités, le chiffrement des données et la surveillance.

Comme les serveurs de segmentation en unités gèrent la plupart des fonctions de sécurité qui protègent l'information sensible qui y est stockée, ils sont susceptibles d'être associés à l'une des catégories de sécurité les plus élevées parmi tous les sous-systèmes de votre architecture de système d'information. Votre organisation devrait évaluer attentivement et tenir à jour la catégorisation de sécurité et le profil de contrôle de sécurité attribués aux serveurs de segmentation en unités. Pour en savoir plus sur les catégories de sécurité, consultez l'ITSP.50.103, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique* [12].

Certaines applications et bases de données comportent des capacités de segmentation en unités intégrées. Le modèle de segmentation en unités comme service (TaaS pour *Tokenization as a Service*) est maintenant offert couramment dans les services infonuagiques. Ces solutions peuvent être avantageuses, car votre organisation n'a alors pas à installer, gérer et entretenir un serveur de segmentation en unités. Selon les exigences liées à vos activités et à la sécurité, et vos capacités en matière de soutien TI, ces solutions pourraient bien répondre à vos besoins. Toutefois, il peut être plus difficile d'évaluer l'efficacité des contrôles et des fonctions de sécurité des solutions de segmentation en unités qui ne sont pas associées à des serveurs de segmentation en unités dédiés. Nous vous recommandons de suivre les trois premières étapes du processus de gestion des risques liés à la sécurité infonuagique présenté dans l'ITSM.50.062 [1] :

1. Effectuer la catégorisation de la sécurité;
2. Sélectionner le profil de contrôle de sécurité approprié;
3. Sélectionner le modèle de déploiement infonuagique et le modèle de services infonuagiques.

Vous devriez passer par ces étapes avant de choisir l'architecture de segmentation en unités qui convient le mieux aux besoins de votre organisation sur le plan des activités et de la sécurité.

3 Considérations liées aux solutions de segmentation en unités

Nos conseils en matière de sécurité infonuagique reposent sur les stratégies de défense en profondeur décrites dans l'ITSP.50.104 [10]. Lorsque vous déterminez les exigences relatives à la sécurité de votre organisation pour les systèmes de segmentation en unités qui prennent en charge vos services fondés sur l'infonuagique, vous devriez également en tenir compte dans le contexte de la défense en profondeur.

Les considérations présentées dans cette section sont regroupées en fonction des couches de défense établies dans l'ITSP.50.104 [10], qui se trouvent à la figure 2.

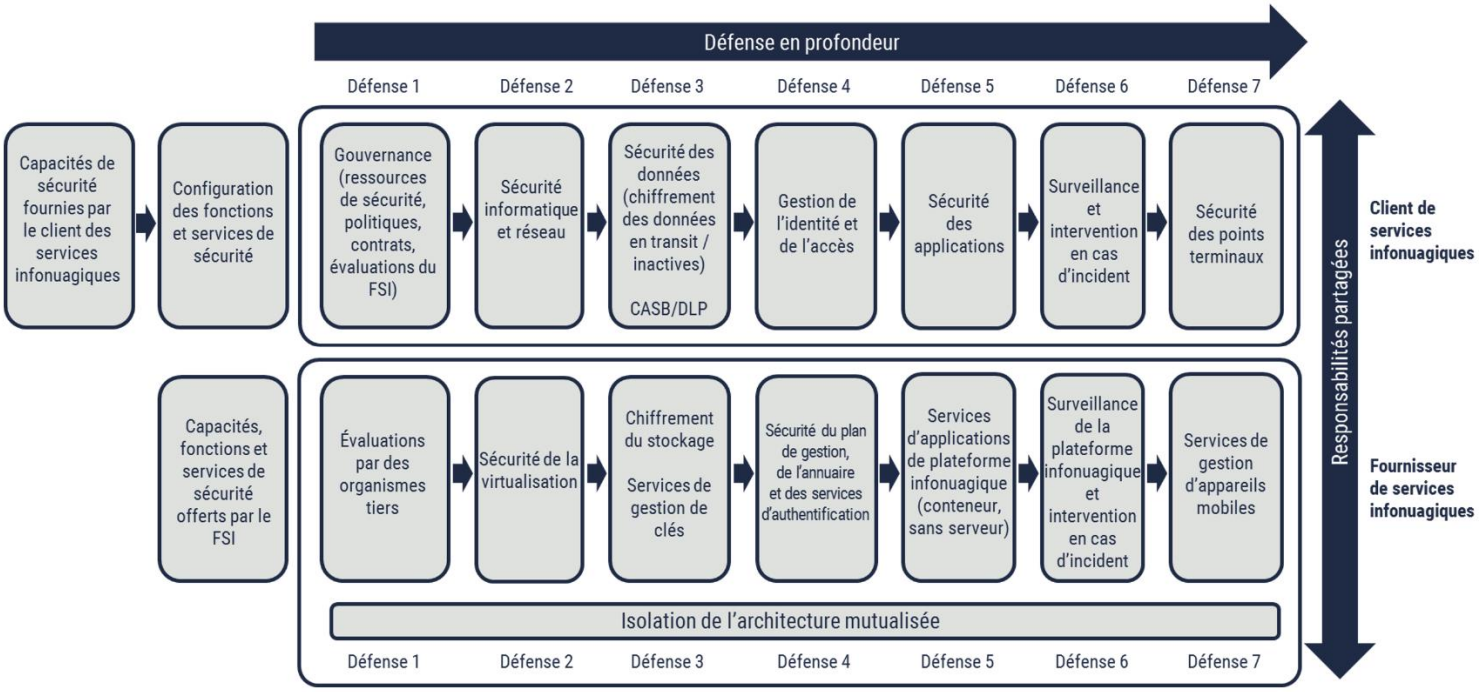

Figure 2 : **La défense en profondeur pour les services fondés sur l'infonuagique**

3.1 Gestion des risques et gouvernance

La stratégie de défense en profondeur du service de segmentation en unités de votre organisation repose sur vos politiques, vos directives, vos exigences contractuelles et l'attribution de vos ressources de sécurité (c'est-à-dire votre cadre de gouvernance). Une gouvernance appropriée permettra à votre organisation de respecter les exigences juridiques et de conformité et d'établir clairement les rôles et les responsabilités connexes. Votre cadre de gouvernance définit les principes directeurs de la protection de l'information sensible confiée à votre organisation.

La première étape du processus de gestion des risques liés à l'infonuagique consiste à réaliser la catégorisation de la sécurité. Dans le cadre de ce processus, votre organisation doit déterminer les lois, les règlements et les normes qui s'appliquent à ses activités et l'information qu'elle utilise pour mener ces dernières. Votre organisation peut se servir de cette évaluation pour déterminer ce qui suit :

- les mesures de sécurité nécessaires pour protéger cette information;
- les valeurs et les champs de données propres à l'information qu'il conviendrait de segmenter en unités dans vos services fondés sur l'infonuagique.

Toutefois, le manque de normes internationales peut poser des défis au moment de mettre en œuvre la segmentation en unités pour protéger l'information sensible. En l'absence de normes d'accréditation des systèmes de segmentation en unités, votre organisation devra évaluer, au moins une fois par année, les mesures de sécurité liées aux systèmes de segmentation en unités qu'elle a choisis. L'évaluation de sécurité initiale et les évaluations ultérieures vous aideront à comprendre l'efficacité globale des contrôles de sécurité ainsi qu'à déterminer et à gérer le risque résiduel.

3.2 Sécurité réseau

Quels que soient les modèles de services infonuagiques et la solution de segmentation en unités que vous choisissez, l'information sensible transite par vos réseaux à mesure qu'elle est recueillie, envoyée au service de segmentation en unités et récupérée par les applications et utilisateurs autorisés (activités 1, 2 et 6 à la figure 1). Pour protéger l'information en transit, vous devez sécuriser les connexions qui relient votre réseau aux services de segmentation en unités et aux services infonuagiques. Vous devez également protéger les connexions réseau utilisées tant pour accéder aux services de segmentation en unités et aux services de sécurité connexes que pour administrer et surveiller ces services.

Pour établir une architecture de sécurité axée sur la défense en profondeur efficace, vous devez segmenter de manière appropriée les réseaux utilisés par le serveur de segmentation en unités et connectés à ce serveur. La segmentation réseau améliore le contrôle de l'accès, la surveillance et le confinement dans l'éventualité d'une compromission. Nous vous recommandons de vous assurer que les services d'information externes, y compris vos systèmes fondés sur l'infonuagique, peuvent joindre le serveur de segmentation en unités uniquement par l'entremise d'une passerelle de sécurité. Vous devriez isoler le serveur de segmentation en unités de l'accès Internet.

Pour obtenir d'autres conseils sur la façon de sécuriser les réseaux associés ou connectés à vos systèmes de segmentation en unités, consultez l'ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau* [13], et l'ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* [14].

3.3 Informatique

Cette couche de défense s'applique à la protection des hôtes physiques, des processeurs, des hyperviseurs, des machines virtuelles et des plateformes qui prennent en charge votre service de segmentation en unités. Pour réduire les risques liés à l'information sensible traitée par ces systèmes, votre organisation devrait mettre en œuvre des pratiques exemplaires en matière de sécurité, comme l'application de correctifs, la configuration de sécurité de base et la surveillance.

L'une des principales considérations liées à la sécurité consiste à maintenir l'isolation entre le service de segmentation en unités et les applications qui accèdent à l'information segmentée en unités. Le risque d'accès non autorisé à l'information sensible s'accroît considérablement si l'isolation n'est pas maintenue (voir la section 7.2.4 de la norme ANSI X9.119-2 [8]). Le moyen le plus direct d'assurer cette isolation consiste à héberger le service de segmentation en unités et les applications connexes sur des systèmes physiques distincts. Si le service de segmentation en unités et les applications qui s'y connectent sont hébergés dans le même environnement informatique, vous pouvez procéder à l'isolation des processus (p. ex. des systèmes d'exploitation distincts), à l'isolation de l'environnement (p. ex. des machines virtuelles distinctes) ou à la séparation des processus physiques (p. ex. des processeurs distincts).

3.4 Sécurité des données

La protection de l'information sensible constitue l'une des principales raisons d'utiliser un service de segmentation en unités. Il est donc essentiel de mettre en œuvre des mécanismes appropriés dans la couche de défense de la sécurité des données afin de réduire le risque résiduel associé à cette information.

Bien que les autres couches de défense jouent un rôle dans la protection de l'information sensible, vous devrez tenir compte de plusieurs considérations propres au stockage et aux bases de données de la segmentation en unités :

- stockage;
- disponibilité;
- réplication et sauvegarde;
- élimination et rémanence des données;
- chiffrement.

3.4.1 Stockage

Le coffre de jetons correspond au système qui stocke les jetons, les valeurs d'origine et l'information sur le mappage des jetons. L'une des premières décisions qu'aura à prendre votre organisation dans le cadre de l'architecture de sécurité concerne l'emplacement du coffre de jetons. Selon les politiques, les règlements et les normes qui s'appliquent à votre organisation, certaines limites sur le plan géographique (p. ex. résidence des données) ou de l'architecture pourraient avoir une incidence sur l'emplacement du coffre de jetons (et de l'information qu'il contient). Si vous utilisez des systèmes de segmentation en unités de tiers ou que vous stockez votre coffre de jetons à l'extérieur de vos installations, vous n'exercez pas un contrôle direct sur l'information sensible qui y est traitée et stockée.

Les coffres de jetons regroupent vraisemblablement une grande partie ou l'ensemble de l'information sensible de votre organisation. On pourrait donc les placer dans une catégorie de sécurité plus élevée que d'autres éléments de votre

architecture de système d'information. Consultez la section 4.3.3.1 de l'ITSP.50.104 [10] pour en savoir plus sur ce regroupement.

Dans le cadre de votre processus de gestion des risques liés à la sécurité, vous devriez choisir l'emplacement de stockage du coffre de jetons en tenant compte de ces considérations et du risque résiduel associé à chaque option d'architecture.

3.4.2 Disponibilité

Si les besoins opérationnels de votre organisation nécessitent l'accès sans interruption aux services de segmentation en unités ou à l'information contenue dans les coffres de jetons, votre architecture de sécurité devra prendre en charge des capacités de haute disponibilité ou de basculement. Vous pouvez établir des capacités de haute disponibilité ou de basculement en utilisant des systèmes dispersés ou redondants.

Si votre organisation a externalisé une partie ou l'ensemble des services de segmentation en unités, vous devriez définir vos exigences en matière de disponibilité dans les contrats et les accords sur les niveaux de service. Assurez-vous que le système ou service de segmentation en unités que vous utilisez répond à vos besoins opérationnels en matière de disponibilité.

3.4.3 Réplication et sauvegarde

Votre organisation devra peut-être se doter de plusieurs systèmes de segmentation en unités pour répondre à ses besoins opérationnels en matière de traitement, d'accès ou de disponibilité. Il est possible que vous deviez synchroniser, gérer et sécuriser les multiples serveurs de segmentation en unités, coffres de jetons et sauvegardes qui se trouvent dans divers emplacements. Quelle que soit l'architecture de sécurité que votre organisation choisit ou conçoit, vous devez vous assurer que l'information sensible qui est transmise entre chaque emplacement et qui y est stockée demeure sécurisée tout au long de son cycle de vie.

3.4.4 Élimination et rémanence des données

Votre organisation est responsable de protéger l'information sensible tout au long de son cycle de vie – lors de la collecte, du stockage, de l'utilisation, de la transmission et de l'élimination une fois qu'elle n'est plus nécessaire. Lorsque vous remplacez ou réutilisez les supports associés aux serveurs de segmentation en unités, aux coffres de jetons et aux sauvegardes, il peut être possible de récupérer une partie de l'information sensible qui était stockée sur le support en question. Vous devriez établir des politiques, des procédures et des ressources pour assurer le nettoyage et l'élimination sécurisés de ces supports.

Pour en savoir plus sur la rémanence des données, consultez la section 4.5.4.5 de l'ITSP.50.104 [10]. Pour en savoir plus sur le nettoyage des supports, consultez l'ITSP.40.006 v2, *Nettoyage des supports de TI* [15].

3.4.5 Chiffrement

Pour protéger efficacement l'information sensible tout au long de son cycle de vie, il importe de la chiffrer lors de sa transmission et de son stockage. Nous vous recommandons de chiffrer périodiquement tous les réseaux et les supports de stockage conformément aux conseils présentés dans l'ITSP.40.111 [14] et l'ITSP.50.106, *Guide sur le chiffrement des services infonuagiques* [16], le cas échéant. Au moment de se doter d'un système de segmentation en unités, votre

organisation devrait s'assurer que les services de chiffrement et de gestion des clés utilisés par ce système sont eux aussi conformes aux recommandations formulées dans ces documents.

3.5 Gestion de l'identité et de l'accès

Il est essentiel de mettre en œuvre des contrôles de l'identification, de l'authentification et de l'accès pour sécuriser le système de segmentation en unités et protéger l'information et les services contenus dans le système. Ces contrôles comportent notamment la séparation des espaces de stockage, la séparation des tâches et les autorisations en fonction du rôle. Consultez les recommandations additionnelles dans l'ITSP.30.031 v3, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* [17], pour vous aider à choisir les contrôles de sécurité appropriés lorsque vous concevez un système d'authentification des utilisateurs.

Pour vous assurer que seuls les utilisateurs, les applications et les systèmes autorisés peuvent accéder à votre système de segmentation en unités, vous devriez déterminer les besoins en matière d'accès (c'est-à-dire les entités qui ont besoin d'y accéder, les types d'accès dont elles ont besoin, l'information et les services auxquels ces entités devront accéder). Par exemple, vous devriez déterminer qui est autorisé à soumettre des données aux fins de la segmentation en unités, à demander la désegmentation des unités et à accéder au plan de gestion du système de segmentation en unités. Nous recommandons également d'intégrer, dans la mesure du possible, les systèmes d'identification et d'authentification (I et A) permettant de contrôler l'accès à votre système de segmentation en unités aux autres systèmes d'I et A utilisés par votre organisation. Votre organisation devrait mettre en œuvre le contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*) pour tous les services du plan de gestion, y compris les fonctions cryptographiques assurées par le serveur de segmentation en unités.

3.6 Applications

Voici quelques considérations liées à la couche de défense des applications relativement à la segmentation en unités :

- développement d'applications sécurisées;
- analyse du code source;
- tests de sécurité et de vulnérabilités;
- déploiement sécurisé;
- gestion des vulnérabilités d'exécution;
- protection contre les menaces.

Dans le contexte des applications de segmentation en unités, la méthode employée pour générer les jetons constitue l'une des principales préoccupations. Il ne devrait pas être possible de désegmenter les unités ni de déterminer la valeur d'origine d'un jeton à l'extérieur de votre système de segmentation en unités. La désegmentation des unités devrait être effectuée uniquement à la demande des utilisateurs, des applications ou des systèmes autorisés. Par conséquent, les organismes de tests indépendants devraient démontrer et valider les méthodes de RNG ou de chiffrement utilisées pour générer les jetons, dans le but de réduire les risques de désegmentation des unités non autorisée et de fuite de l'information sensible connexe.

3.7 Surveillance et intervention en cas d'incident

Votre organisation devrait avoir recours à des capacités de surveillance de la sécurité et d'intervention en cas d'incident afin de maintenir et d'adapter son architecture de sécurité de l'information et ses pratiques en fonction de l'évolution des menaces. Nous vous recommandons d'envisager l'adoption d'un modèle de sécurité qui anticipe une atteinte à la sécurité. Vous devriez affecter les ressources nécessaires en matière de sécurité pour détecter et définir les attaques d'auteurs malveillants et les vulnérabilités découvertes dans vos systèmes d'information, et intervenir en conséquence. Les coûts liés à l'atténuation d'une atteinte à la sécurité et à la fuite d'information sensible dépassent souvent largement les coûts liés à la mise en place de capacités efficaces de surveillance de la sécurité de l'information et de réponse aux menaces.

Votre système de segmentation en unités devrait permettre et faciliter le suivi, la surveillance et la journalisation de tout accès au système et aux services de sécurité pris en charge et de toute action prise dans ce système et ces services. Les services de surveillance devraient détecter toute défaillance et anomalie ou tout comportement suspect, puis transmettre des alertes à la direction et au personnel de sécurité. La direction et le personnel de sécurité de votre organisation peuvent se servir de ces alertes et analyser les journaux connexes afin de détecter et d'atténuer proactivement les problèmes, les vulnérabilités et les compromissions touchant vos systèmes de segmentation en unités.

3.8 Sécurité des points terminaux

En plus de mettre en œuvre des mesures et des contrôles de sécurité visant à protéger le système de segmentation en unités et les réseaux qui y sont connectés, votre organisation devrait protéger tous les systèmes et les dispositifs autorisés à accéder à l'information sensible d'origine. Si des auteurs de menace réussissaient à compromettre ces systèmes ou dispositifs, ils pourraient obtenir un accès non autorisé au système de segmentation en unités. Ils pourraient également utiliser l'information stockée dans ces dispositifs pour créer des tables arc-en-ciel et lancer des attaques par force brute ou

par réinsertion. Au moyen de ces vecteurs d'attaque, les auteurs de menace pourraient désegmenter les unités et accéder à l'information sensible segmentée en unités qui est stockée dans des systèmes d'information ouverts ou moins sécurisés.

4 Sommaire

Le présent document fournit des conseils sur les facteurs liés à la défense en profondeur et à l'architecture de sécurité dont il faut tenir compte pour mettre en œuvre, exploiter et gérer avec efficacité le système de segmentation en unités de votre organisation.

Votre organisation peut appliquer la segmentation en unités afin de protéger la confidentialité et l'intégrité de l'information sensible transmise, stockée et traitée par des systèmes fondés sur l'infonuagique. La segmentation en unités peut également aider votre organisation à se conformer aux politiques, aux règlements et aux normes qui régissent ses activités. Il convient toutefois de souligner que la segmentation en unités doit s'inscrire dans une architecture de sécurité axée sur la défense en profondeur. Vous devriez également vous assurer que la segmentation en unités est prise en charge par les autres technologies de sécurité que vous utilisez, comme le chiffrement.

4.1Coordonnées et assistance

Pour obtenir de l'information supplémentaire sur la mise en œuvre de la segmentation en unités dans le but de protéger l'information sensible ou des renseignements personnels, veuillez communiquer avec notre centre d'appel :

Centre d'appel
contact@cyber.gc.ca
613-949-7048

5 Contenu complémentaire

5.1 Abréviations, acronymes et sigles

Forme abrégée	Expression au long
ANSI	American National Standards Institute
FSI	Fournisseur de services infonuagiques
FPE	Chiffrement préservant le format (*Format-Preserving Encryption*)
GC	Gouvernement du Canada
I et A	Identification et authentification
TI	Technologies de l'information
NIST	National Institute of Standards and Technology
PCI DSS	Normes de sécurité sur les données de l'industrie des cartes de paiement (*Payment Card Industry Data Security Standard*)
LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques
PRNG	Générateur de nombres pseudo-aléatoires (*Pseudo-Random Number Generator*)
RNG	Générateur de nombres aléatoires (*Random Number Generator*)
CDS	Cycle de développement des systèmes
TaaS	Segmentation en unités comme service (*Tokenization as a Service*)
TLP	Protocole TLP (*Traffic Light Protocol*)

5.2 Glossaire

Terme	Définition
Modèle de sécurité qui anticipe une atteinte à la sécurité	Stratégie de sécurité de l'information consistant à supposer que les systèmes d'information sont déjà compromis, mais que la compromission n'a pas encore été détectée.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin.
Fournisseur de services infonuagiques	Fournisseur commercial de services infonuagiques qui souhaite offrir ses services à des clients.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Résidence des données	Emplacement physique ou géographique des données numériques au repos d'une organisation.
Déchiffrement	Opération par laquelle un texte chiffré est rétabli en texte en clair.
Défense en profondeur	Stratégie de sécurité de l'information intégrant les personnes, la technologie et les capacités opérationnelles pour établir des barrières variables dans de multiples couches et dimensions de l'organisation.
Désegmentation des unités	Processus qui inverse la segmentation en unités en restaurant les données ou l'information d'origine qui avait été mappée à un jeton.
Chiffrement	Opération par laquelle une information est transformée d'un texte en clair à un texte chiffré afin d'en dissimuler le contenu et d'empêcher tout accès non autorisé.
Chiffrement préservant le format	Technique de chiffrement selon laquelle la sortie conserve le format de l'information d'origine.
Identification et authentification	Processus consistant à établir l'identité d'une entité qui interagit avec un système.
Intégrité	Capacité à protéger l'information contre une modification ou une suppression non autorisée.
Renseignement personnel	Tout renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable.
Générateur de nombres pseudo-aléatoires	Processus servant à générer des séquences de nombres présentant certaines propriétés du hasard.
Générateur de nombres aléatoires	Processus servant à générer une séquence de valeurs aléatoires (normalement une séquence de bits) ou une valeur individuelle au hasard.
Risque résiduel	Degré de probabilité et répercussions potentielles d'une menace qui subsistent après la mise en application des contrôles de sécurité.

Terme	Définition
Gestion des risques	Démarche systématique visant à établir la meilleure façon de procéder dans des circonstances incertaines par la détermination, l'évaluation, la compréhension et la communication des questions liées aux risques, de même que par la prise de décisions conséquentes.
Nettoyage	Processus consistant à retirer les données d'un support avant de réutiliser ce support dans un environnement dont le niveau de protection n'est pas acceptable pour les données qui s'y trouvaient avant le nettoyage.
Catégorisation de la sécurité	Processus permettant d'identifier le préjudice potentiel lié à la compromission des processus opérationnels et de l'information connexe, et de déterminer la catégorie de sécurité correspondante.
Profil de contrôle de sécurité	Ensemble de contrôles et d'améliorations de sécurité qui, lorsqu'il est mis en œuvre de manière appropriée dans le contexte des techniques et des menaces propres à une organisation, permet de protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information appuyant les activités opérationnelles.
Information sensible	Information qui doit être protégée contre toute divulgation non autorisée.
Segmentation en unités	Processus consistant à générer une valeur de remplacement (appelée jeton) et à substituer celle-ci à l'information ou aux données d'origine.
Coffre de jetons	Système qui stocke les jetons, les valeurs d'origine et l'information sur le mappage des jetons.

5.3 Références

Numéro	Référence
1.	Centre canadien pour la cybersécurité. *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)*, mars 2019.
2.	Centre canadien pour la cybersécurité. *Modèles de l'infonuagique (ITSAP.50.111)*, novembre 2018.
3.	Ministère de la Justice Canada. *Loi sur la protection des renseignements personnels*, 1985.
4.	Ministère de la Justice Canada. *Loi sur la protection des renseignements personnels et les documents électroniques*, 2000.
5.	Secrétariat du Conseil du Trésor du Canada. *Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS)*, 1er novembre 2017.
6.	Commissariat à la protection de la vie privée du Canada. *L'infonuagique pour les petites et moyennes entreprises*, juin 2012.
7.	Industrie des cartes de paiement. *Normes de sécurité des données de l'industrie des cartes de paiement* , version 3.2.1, mai 2018.
8.	American National Standards Institute. *ASC/X9 – ANSI X9.119-2 - Requirements for Protection of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*, 3 août 2017.
9.	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie (ITSG-33)*, novembre 2012.
10.	Centre canadien pour la cybersécurité. *Guide sur la défense en profondeur pour les services fondés sur l'infonuagique (ITSP.50.104)*, mai 2020.
11.	National Institute of Standards and Technology (NIST). *Special Publication 800-38G* Recommendation for Block Cypher Modes of Operation: Methods for Format-Preserving Encryption, mars 2016.
12.	Centre canadien pour la cybersécurité. *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103)*, mai 2020.
13.	Centre canadien pour la cybersécurité. *Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062)*, août 2020.
14.	Centre canadien pour la cybersécurité. *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)*, août 2016.
15.	Centre canadien pour la cybersécurité. *Nettoyage des supports de TI (ITSP.40.006)*, juillet 2017.
16.	Centre canadien pour la cybersécurité. *Guide sur le chiffrement des services infonuagiques (ITSP.50.106)*, mai 2020.
17.	Centre canadien pour la cybersécurité. *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)*, avril 2018.