Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI : Nº 9, Isoler les applications Web

SÉRIE GESTIONNAIRES

ITSM.10.099

Canada

Avant-propos

L'ITSM.10.099, *Les 10 mesures de sécurité des TI : Nº 9, Isoler les applications Web*, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Il fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées par le Centre pour la cybersécurité dans l'ITSM.10.189, *Les 10 mesures de sécurité des technologies de l'information visant à protéger les réseaux Internet et l'information* [1][1]. Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

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 09 mars 2023.

Historique des révisions

Version	Modifications	Date
1	Première version	09 mars 2023

[1] Les numéros entre les crochets renvoient à des références figurant à la section Contenu complémentaire du présent document.

Vue d'ensemble

L'une des 10 mesures de sécurité des TI recommandées par le CST consiste à isoler les applications Web. On entend par « application Web » tout programme auquel on peut accéder à partir d'Internet et qui utilise des technologies et navigateurs Web pour exécuter des tâches. On pense par exemple aux services de courrier, aux logiciels de traitement de texte, aux convertisseurs de fichiers en ligne et aux calendriers. Les applications Web peuvent également comprendre des appareils de l'Internet des objets (IdO) tels que les caméras de sécurité et les thermostats intelligents. Les données que vous entrez dans ces applications peuvent être stockées dans un environnement local, infonuagique ou hybride. Bien qu'elles soient accessibles lorsque vous en avez besoin, elles peuvent exposer votre organisation à des cyberattaques.

Le présent document traite de plusieurs pratiques exemplaires liées à l'isolement des applications Web dans le but d'assurer la protection des réseaux et des systèmes de votre organisation contre les cybermenaces courantes. L'isolement des applications Web fait partie de la stratégie de défense en profondeur. Les conseils formulés dans la présente sont fondés sur les contrôles de sécurité mentionnés dans l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2].

En isolant les applications Web, vous pouvez réduire votre degré d'exposition aux menaces courantes et protéger les systèmes et réseaux de votre organisation. Ce document met l'accent sur les contrôles de sécurité que vous pouvez mettre en œuvre pour isoler les applications Web. Pour une protection optimale contre les cybermenaces visant les applications Web, votre organisation devrait déployer des mesures de sécurité supplémentaires.

La présente publication fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.189 [1]. Bien que la mise en œuvre de l'ensemble des 10 mesures de sécurité recommandées puisse rendre votre organisation moins vulnérable aux cybermenaces, vous devriez examiner les activités que vous menez sur le plan de la cybersécurité pour déterminer s'il convient de prendre des mesures supplémentaires. Pour de plus amples renseignements sur la mise en œuvre des 10 mesures de sécurité des TI, communiquez par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

D97-4/10-099-2023F-PDF
978-0-660-48021-3

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Aperçu de la gestion des risques liés à la sécurité des TI

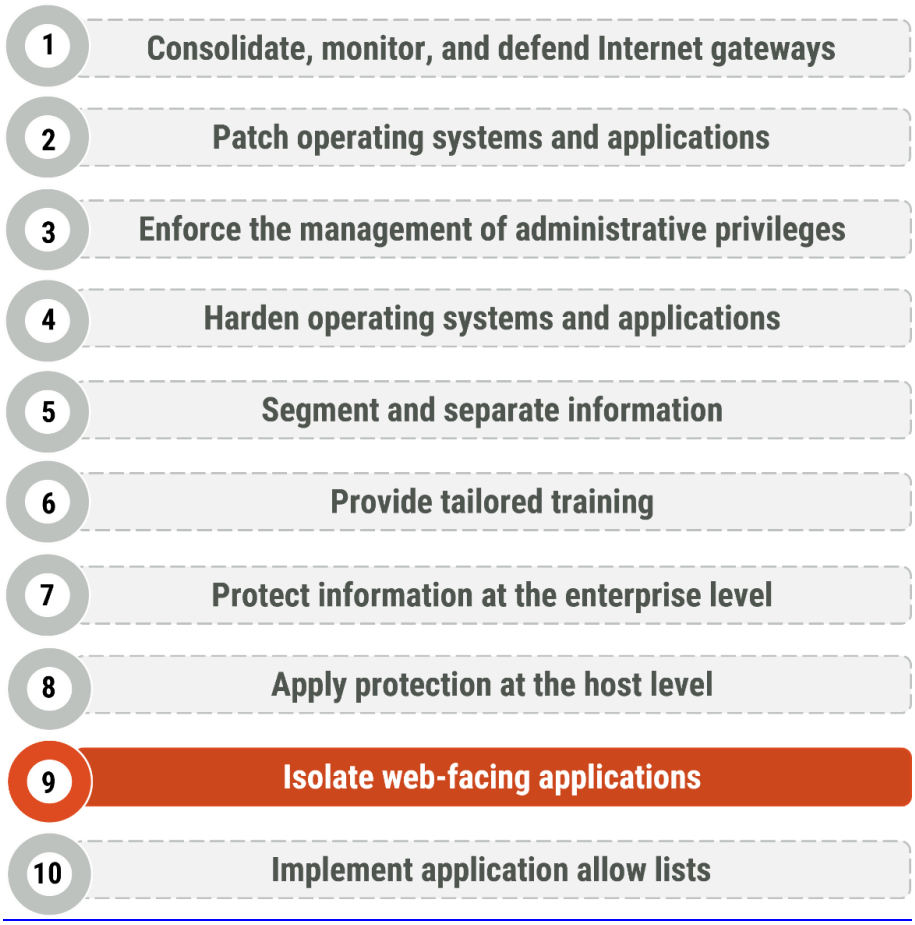
1.1 Les 10 mesures de sécurité des TI

Le présent document fournit des conseils sur l'isolement des applications Web en ayant recours à des technologies de virtualisation. Isoler ces applications permet de réduire le degré d'exposition de votre organisation aux cybermenaces courantes qui touchent les applications Web et qui pourraient compromettre vos réseaux, systèmes et biens de TI.
La présente est fondée sur les conseils et les contrôles de sécurité formulés respectivement dans l'ITSM.10.189 [1] et l'annexe 3A de l'ITSG-33 [2].

Les 10 mesures de sécurité des TI recommandées par le CST qui sont mentionnées à la figure 1 ci-dessous et dans l'ITMS.10.189 [1] sont fondées sur une analyse des tendances inhérentes aux cybermenaces et sur les répercussions de telles menaces sur les réseaux connectés à Internet. La mise en œuvre de toutes les mesures permettra de corriger la plupart des vulnérabilités liées à la sécurité des TI qui pèsent sur votre organisation.

Les cybermenaces peuvent entraîner diverses répercussions en fonction de l'environnement opérationnel et technique de votre organisation. Pour satisfaire vos besoins en matière de sécurité, vous devez examiner les activités menées actuellement par votre organisation sur le plan de la sécurité et de la gestion des risques.

Figure 1 : Les 10 mesures de sécurité des TI – Nº 9, Isoler les applications Web



1.2 Rapport avec le processus de gestion des risques liés à la sécurité des TI

Les 10 mesures de sécurité des TI du CST découlent des contrôles de sécurité mentionnés à l'annexe 3A de l'ITSG-33 [2]. L'ITSG-33 [2] décrit les rôles, les responsabilités et les activités qui permettent à une organisation de gérer les risques relevant de la sécurité des TI, et comprend un catalogue de contrôles de sécurité (c.-à-d. un ensemble standardisé d'exigences de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI). Il existe trois classes de contrôles de sécurité qui sont subdivisées en plusieurs familles de contrôles de sécurité connexes :

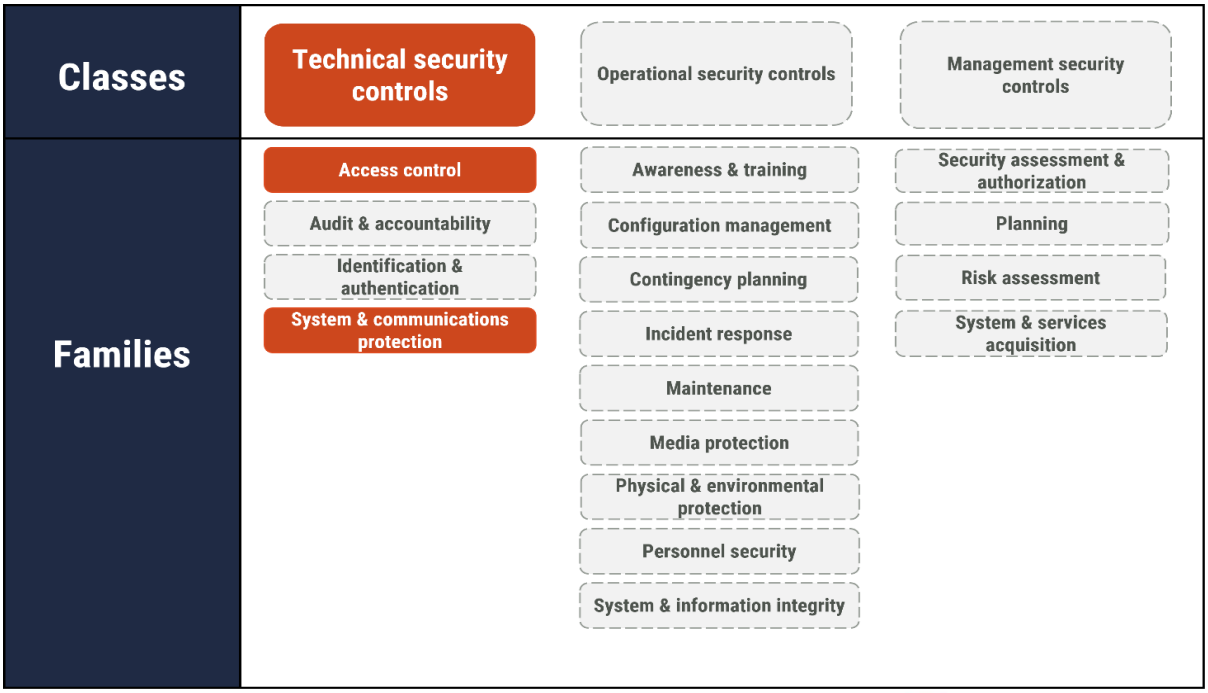
- **Contrôles de sécurité techniques :** contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels;
- **Contrôles de sécurité opérationnels :** contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies comme les logiciels de soutien;
- **Contrôles de sécurité de gestion :** contrôle de sécurité qui porte principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.

Tel qu'il est illustré dans la figure 2, le présent document fait mention de mesures qui appartiennent aux familles de contrôles Contrôle d'accès (AC pour *Access Control*) et Protection des systèmes et des communications (SC pour *System and Communications Protection*). Le présent document décrit les contrôles suivants :

- **AC-6 Droit d'accès minimal**
- **SC-32 Partitionnement des systèmes d'information**

De plus amples renseignements sur les contrôles AC-6 et SC-32 sont fournis à l'annexe A du présent document.

Figure 2 : Classes et familles de contrôles de sécurité applicables décrites dans l'ITSG-33



Vous pouvez utiliser les contrôles de sécurité mentionnés dans le présent document et à l'annexe 3A de l'ITSG-33 [2] pour déterminer la meilleure façon de gérer les risques liés à la cybersécurité de votre organisation et protéger ses réseaux, ses systèmes et ses biens de TI. Il convient toutefois de garder à l'esprit que la mise en œuvre de ces contrôles ne constitue qu'une partie du processus de gestion des risques liés à la sécurité des TI.

L'ITSG-33 [2] décrit un processus fondé sur deux niveaux d'activités de gestion des risques, à savoir les activités menées au niveau organisationnel et les activités menées au niveau du système d'information. Ces deux niveaux d'activités vous aideront à déterminer les besoins en matière de sécurité pour l'ensemble de votre organisation et pour ses systèmes d'information. Après avoir compris vos besoins pour chaque niveau, vous serez en mesure d'établir les contrôles de sécurité que votre organisation doit mettre en place et maintenir pour satisfaire un niveau de risque acceptable.

Remarque : Les contrôles de sécurité et pratiques exemplaires mentionnés dans la présente ne sont pas décrits en détail. Comme pour toute solution de TI, votre organisation doit passer en revue ses exigences opérationnelles et en matière de sécurité afin de déterminer la meilleure façon d'adapter votre approche en matière de sécurité.

2 Menaces touchant les applications Web

Cette section présente un sommaire des menaces courantes visant les applications Web. L'isolement de toutes les applications Web est l'une des mesures essentielles que vous pouvez prendre pour réduire le degré d'exposition de votre organisation aux cybermenaces.

Par « application Web », on entend tout programme auquel on peut accéder au moyen d'une connexion réseau et qui utilise des technologies et navigateurs Web pour exécuter des tâches sur Internet, notamment les services de courrier, les logiciels de traitement de texte, les convertisseurs de fichiers, les solutions de commerce électronique, les calendriers ou les appareils IdO. Les applications Web sont pratiques et rentables. Les données associées à ces applications peuvent être stockées dans un environnement local, infonuagique ou hybride, ce qui les rend accessibles en tout temps. Par ailleurs, les applications Web peuvent servir à améliorer les processus opérationnels et à appuyer le télétravail. Généralement, elles sont faciles à installer et à maintenir puisque les correctifs et mises à jour peuvent être déployés sur les appareils à distance.

Cependant, la sécurité est souvent reléguée au second plan lors de la conception des applications. Si des mesures de sécurité ne sont pas intégrées aux applications, celles-ci peuvent être vulnérables aux accès non autorisés, aux fuites de données et à d'autres problèmes de sécurité. Des défauts ou lacunes dans le code peuvent également fragiliser les applications, surtout face à des attaques par script intersites (XSS pour *Cross-Site Scripting*) ou par injection SQL (*Structured Query Language*).

2.1 Compréhension des menaces courantes

Les auteures et auteurs de cybermenace cherchent à modifier les paramètres des applications et à exécuter des fonctionnalités non autorisées ou malveillantes sur les applications. En exploitant les vulnérabilités des applications, les auteures et auteurs de menace peuvent obtenir un accès non autorisé à des renseignements de nature délicate, comme des renseignements personnels ou commerciaux, qui sont conservés dans les applications Web ou qui sont traités par celles-ci. Les attaques contre les applications Web peuvent entraîner une exposition d'information, un vol d'identité, une compromission de l'application ou d'autres systèmes organisationnels, ou un déni de service.

Le tableau 1 présente des exemples de menaces courantes pesant sur les applications Web, y compris la méthode d'attaque et l'incidence que l'attaque pourrait avoir sur votre organisation et les utilisateurs de l'application. Cette information s'appuie sur la publication *Top 10 – 2021* [3] de l'Open Web Application Security Project (OWASP). Il convient de noter que cette liste de menaces n'est pas exhaustive.

Tableau 1 : Menaces courantes touchant les applications Web

Menace	Méthode	Incidence potentielle
Contrôle d'accès défaillant	Les auteures et auteurs de menace exploitent les vulnérabilités dans l'application du contrôle d'accès, telles que l'omission de mettre en œuvre le principe de droit d'accès minimal ou d'examiner les droits d'administrateur et de les modifier au besoin.	Le contrôle d'accès applique la politique de façon à bloquer toute action des utilisateurs au-delà de leurs autorisations prévues. Les échecs de contrôle d'accès mènent

Menace	Méthode	Incidence potentielle
	Les vecteurs d'attaque courants comprennent la violation du principe de droit d'accès minimal ou de refus par défaut, la falsification de paramètres ou la navigation forcée (contourner les contrôles d'accès en modifiant l'URL ou la page HTML), et la manipulation de métadonnées.	souvent à une divulgation non autorisée d'information, à la modification des données, à la destruction de toutes les données ou à l'exécution d'une fonction opérationnelle qui dépasse les restrictions imposées à l'utilisateur.
Attaque par script intersites (XSS)	Un auteur ou auteure de menace injecte des scripts malveillants dans une application Web bénigne et de confiance. Il utilise l'application pour transmettre du code malveillant, qui prend souvent la forme de scripts côté navigateur, à quiconque utilise l'application.	L'appareil de l'utilisateur devient infecté par du code malveillant qui peut accéder à des témoins de connexion, à des jetons de session ou à d'autres informations de nature délicate qui sont conservées par l'application.
Attaque par injection SQL	Les auteures et auteurs de menace ajoutent du code SQL dans les données d'entrée pour nuire à l'exécution de commandes SQL prédéfinies.	Les auteures et auteurs de menace peuvent supprimer, modifier ou consulter des données de nature délicate, ou encore exécuter des opérations d'administrateur.
Attaque par injection de commande	Un auteur ou auteure de menace utilise une faille pour transmettre du code malveillant d'une application Web à un autre système.	L'auteure ou auteur de menace peut prendre le contrôle de l'application.
Dépassement de mémoire tampon	Un auteur ou auteure de menace envoie de grandes quantités de données qui excèdent les quantités attendues par l'application, ce qui l'empêche de fonctionner normalement.	L'auteure ou auteur de menace peut exécuter des commandes ou des programmes et accéder aux systèmes.
Attaque par force brute	Un auteur ou auteure de menace tente de deviner l'information d'authentification par essais-erreurs afin d'obtenir l'accès au compte ciblé et à ses données. Il peut utiliser un logiciel automatisé pour soumettre de nombreux mots de passe de façon consécutive, en espérant tomber sur le bon.	L'auteure ou auteur de menace parvient à accéder au compte d'un utilisateur et à toutes les informations de nature délicate associées au compte (p. ex. information de carte de crédit stockée).

Menace	Méthode	Incidence potentielle
Attaque par traversée de chemin	Les auteures et auteurs de menace utilisent cette attaque, que l'on appelle également attaque par traversée de répertoire, pour accéder aux fichiers et aux répertoires stockés en dehors du dossier racine Web. Ils se servent de variables, comme les séquences point, point, barre oblique (../), pour monter dans la hiérarchie du répertoire.	Un auteur ou auteure de menace peut accéder au code source des applications, aux informations d'identification de l'utilisateur, aux bases de données ou aux fichiers sur la configuration et les systèmes essentiels.
Exploitation d'une vulnérabilité d'inclusion de fichier	Un auteur ou auteure de menace contrôle quel fichier est exécuté au moment de l'exécution, en ayant recours à une variable afin de construire un chemin vers le code exécutable. Cette attaque touche habituellement les applications qui dépendent de la durée d'exécution du script.	L'auteure ou auteur de menace peut utiliser l'exécution de code distant pour exécuter une application ou créer un interpréteur de commandes Web sur le serveur Web en vue d'exécuter des commandes à distance de façon interactive.
Attaque par falsification de requête côté serveur (SSRF pour *Server-Side Request Forgery*)	Cette attaque exploite une application Web qui obtient une ressource distante sans valider l'URL fournie par l'utilisatrice ou utilisateur. L'auteure ou auteur de menace peut contraindre l'application à envoyer une requête élaborée à une destination inattendue, même si elle est protégée par un pare-feu, par un réseau privé virtuel (RPV) ou par un autre type de liste de contrôle d'accès (LCA) au réseau.	Vos systèmes peuvent être ciblés même s'ils se trouvent derrière des pare-feux ou des LCA réseau. Comme la plupart des applications Web modernes offrent aux utilisatrices et utilisateurs finaux des fonctions pratiques, la récupération d'une URL devient un scénario courant. L'auteure ou auteur de menace pourrait analyser les ports afin de trouver ceux qui sont ouverts, accéder à des données de nature délicate, accéder au stockage des métadonnées des services infonuagiques ou mener une attaque par déni de service (DoS pour *Denial of Service*). La gravité des attaques par SSRF augmente en raison des services en nuage et de la complexité des architectures.

3 Contrôles de sécurité pour les applications Web

Cette section décrit les mesures que votre organisation peut prendre lorsqu'elle isole les applications Web. Ces mesures sont fondées sur les contrôles de sécurité **SC-32 Partitionnement des systèmes d'information** et **AC-6 Droit d'accès minimal**. Pour obtenir de plus amples renseignements sur ces contrôles, veuillez consulter les annexes A.1 et A.2 du présent document.

Bien que les contrôles de sécurité ci-dessous soient un bon point de départ pour protéger votre organisation, vous devriez également songer à prendre les mesures suivantes :

- analyser et tester les applications pour détecter les vulnérabilités;
- appliquer les correctifs et les mises à jour aux applications dès qu'ils sont publiés;
- mettre en place une liste d'applications autorisées;
- mettre en œuvre des pare-feux d'applications Web.
    - Il existe deux différents types de pare-feux d'applications : les pare-feux d'applications au niveau du réseau et les pare-feux d'applications au niveau de l'hôte. Les deux fournissent une barrière qui empêche que l'on accède aux ressources des systèmes locaux de l'extérieur.

Pour en savoir plus au sujet des mesures ci-dessus, veuillez consulter l'ITSM.10.095, *Les 10 mesures de sécurité des TI : Nº 10, Mettre en place une liste d'applications autorisées* [4] et l'ITSM.10.096, *Les 10 mesures de sécurité des TI : Nº 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications* [5].

3.1 Partitionnement des systèmes d'information (SC-32)

Votre organisation devrait isoler les applications Web afin qu'elles soient hébergées dans des domaines ou environnements distincts et pour réduire les risques de compromission des principaux systèmes d'information et réseaux. L'accès au réseau et la communication avec d'autres composants de système d'information sont restreints ou bloqués pour les applications isolées. Si une application isolée est infectée par un maliciel ou compromise, l'exploit sera contenu et ne pourra pas se propager au-delà de l'environnement isolé, également appelé « bac à sable », pour infecter d'autres hôtes ou systèmes.

La segmentation de vos réseaux en zones de sécurité permet d'isoler les applications Web et de protéger les systèmes et les données de votre organisation. La segmentation réduit le degré d'exposition de votre organisation aux menaces qui pourraient exploiter des vulnérabilités publiques et compromettre vos réseaux, vos systèmes et vos biens de TI.

Par « segmentation réseau », on entend une technique de réseau qui divise un réseau en sous-réseaux distincts de plus petite taille, ce qui permet ainsi à une organisation de compartimenter le réseau et de fournir des services et des contrôles de sécurité uniques à chaque sous-réseau. Les zones de sécurité de réseau sont des regroupements logiques qui sont basés sur la mise en œuvre sous-jacente de la segmentation réseau. Les contrôles de sécurité uniques qui protègent une zone sont définis dans le point d'interface de zone (PIZ).

Un PIZ est un système qui contrôle le flux d'information entre deux zones. La différenciation entre les zones se nomme la frontière. La frontière contient des PIZ qui représentent les seuls points de connexion entre les zones. Toutes les données

doivent être transmises d'une zone à une autre par un PIZ, lequel connecte exclusivement ces deux zones et crée un chemin de communication distinct.

Un PIZ en nuage sert à décrire l'interface contrôlée qui relie deux zones. D'autres mécanismes de segmentation logiques peuvent être employés dans un environnement en nuage. Même s'ils ne répondent pas nécessairement à toutes les exigences fonctionnelles de sécurité d'un PIZ, ces mécanismes peuvent jouer un rôle dans l'établissement de zones dans les réseaux.

Les ressources infonuagiques sont déployées dans ces zones précises. Dans un environnement réseau traditionnel, il serait normal d'avoir un PIZ à la frontière de la zone. Dans un environnement en nuage, un PIZ peut être situé à la frontière d'une zone ou dans une zone associée à des interfaces réseau de ressources infonuagiques précises, comme une machine virtuelle (MV) ou un hôte.

3.1.1 Virtualisation

La virtualisation est un moyen courant d'isoler les applications Web. La virtualisation des postes de travail est une technologie qui fait appel aux logiciels pour créer des versions logicielles des systèmes et des services de TI qui sont habituellement mis en œuvre sur du matériel physique distinct. Ces versions logicielles (ou instances virtuelles) peuvent accroître l'efficacité et réduire les coûts de façon considérable. Vous pouvez utiliser le matériel au maximum de sa capacité en répartissant ses fonctionnalités entre plusieurs services différents.

La virtualisation des postes de travail sépare le poste de travail logique de l'appareil physique. L'utilisatrice ou utilisateur interagit avec l'ordinateur hôte en utilisant un autre poste de travail ou appareil mobile qui est connecté au réseau de votre organisation. En ce qui a trait aux applications, vous pouvez utiliser les postes de travail virtuels pour contrôler de façon centralisée les applications auxquelles les utilisatrices et utilisateurs peuvent accéder sur leurs postes de travail.

À l'aide de technologies de virtualisation, vous pouvez encapsuler une application pour la séparer d'autres programmes ou du système d'exploitation sur lequel elle est exécutée. Même si l'application fonctionne toujours comme prévu, elle n'est pas installée sur l'hôte.

3.1.1.1 Machine virtuelle (MV)

La virtualisation permet d'exécuter vos applications tout en utilisant moins de serveurs physiques. Les applications et les logiciels s'exécutent virtuellement sur un système informatique simulé que l'on appelle une machine virtuelle (MV). Une MV est l'équivalent émulé d'un système informatique qui s'exécute sur un autre système. En utilisant une MV, vous pouvez exécuter des applications dans des environnements isolés. Vous pourriez également employer un conteneur, qui est un processus isolé, et non une machine indépendante complète. Lors de l'utilisation d'un conteneur, les applications peuvent s'exécuter dans des espaces utilisateur isolés comme une MV. Toutefois, contrairement aux MV, chaque conteneur partage le système d'exploitation du même hôte sous-jacent et est situé sur un serveur physique.

La VM possède toutes les caractéristiques d'un serveur informatique, sans qu'il soit nécessaire d'y connecter du matériel, et elle est prise en charge par un hyperviseur.

3.1.1.2 Hyperviseur

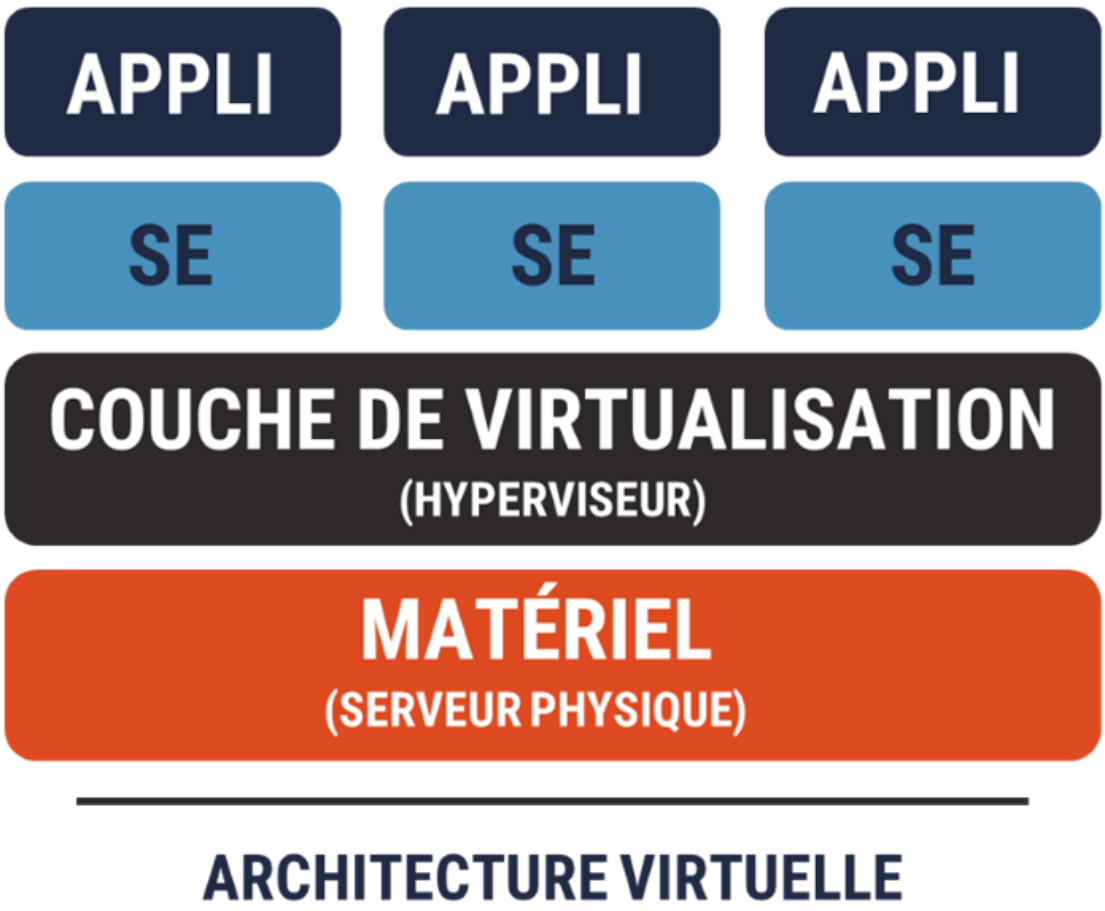
L'hyperviseur est un logiciel qui fournit les ressources informatiques (p. ex. stockage, mémoire) nécessaires pour exécuter virtuellement plusieurs MV.

On retrouve deux types d'hyperviseurs : un hyperviseur sans système d'exploitation et un hyperviseur hébergé.
Un **hyperviseur sans système d'exploitation** s'exécute directement sur le matériel physique, tandis qu'un **hyperviseur hébergé** s'exécute en tant qu'application sur le système d'exploitation d'un hôte.

3.1.1.3 Serveurs matériels

Un seul serveur matériel peut prendre en charge plusieurs MV. Sans la virtualisation, les applications inactives accaparent des ressources qu'elles n'utilisent pas, comme la puissance de traitement, la mémoire RAM ou le stockage. La virtualisation permet d'utiliser les serveurs matériels au maximum de leurs capacités et de fournir à l'hyperviseur toutes les ressources nécessaires pour la prise en charge des MV.

Figure 3 : Environnement virtualisé



3.2 Application du principe du droit d'accès minimal (AC-6)

Votre organisation devrait appliquer le principe du droit d'accès minimal. Essentiellement, ce principe signifie que vous n'accordez à un utilisateur ou utilisatrice que les autorisations d'accès dont il a besoin pour accomplir les tâches autorisées. Ce principe permet de limiter les dommages pouvant résulter de l'utilisation accidentelle, incorrecte ou non autorisée d'une application.

Lorsque vous déployez une application, vous devriez vous assurer que les utilisatrices et utilisateurs détiennent seulement le niveau d'accès dont ils ont besoin pour le fonctionnement de l'application. Les fonctions administratives devraient se limiter aux personnes qui ont besoin de ce niveau de privilège. Vous pourriez considérer la création de processus, de rôles et de comptes de système d'information additionnels, au besoin, pour maintenir le principe du droit d'accès minimal. Vous devriez également utiliser ce principe pour accorder un accès à distance à vos appareils.

Dans les environnements infonuagiques natifs, une posture de sécurité forte et une gestion robuste de l'identité et de l'accès (GIA) sont interreliées. Pour le service de GIA de la zone de gestion (ZG) en nuage, les organisations doivent mettre en œuvre le contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*) afin de pouvoir contrôler les autorisations accordées aux utilisatrices et utilisateurs, et aux ressources. Le contrôle d'accès basé sur les rôles devrait être structuré de façon à appliquer le principe du droit d'accès minimal. La zone de gestion en nuage est un réseau d'administration dédié et isolé que peuvent utiliser les administratrices et administrateurs réseau pour configurer et surveiller les infrastructures réseau.

L'utilisation de domaines de traitement séparés vous permet d'accorder des droits d'accès aux utilisatrices et utilisateurs de façon plus précise. Par exemple, vous pouvez avoir recours à des techniques de virtualisation pour permettre à un utilisateur ou utilisatrice d'avoir des droits d'accès additionnels lorsqu'il utilise une machine virtuelle, et des droits d'accès limités dans d'autres environnements.

Résumé

L'une des 10 mesures de sécurité des TI recommandées par le CST consiste à isoler les applications Web. Pour ce faire, nous recommandons la virtualisation afin de créer un environnement séparé pour les applications, et la mise en œuvre du principe de droit d'accès minimal pour tous les utilisateurs et utilisatrices des applications. Les conseils présentés dans le présent document sont basés sur les contrôles de sécurité AC-6 et SC-32, qui sont décrits en détail à l'annexe A ci-dessous.

L'isolement des applications Web empêche les maliciels de se propager dans d'autres hôtes et systèmes. Cependant, cette mesure n'est qu'un des nombreux éléments nécessaires pour améliorer la cybersécurité de votre organisation. Pour mieux protéger votre organisation contre les cybermenaces, vous devriez passer en revue et mettre en place l'ensemble des mesures recommandées dans l'ITSM.10.189, *Les 10 mesures de sécurité des technologies de l'information visant à protéger les réseaux Internet et l'information* [1].

L'ITSM.10.095, *Les 10 mesures de sécurité des TI : Nº 10, Mettre en place une liste d'applications autorisées* [4] contient de plus amples renseignements sur la sécurité des applications, ainsi que des conseils sur la création d'une liste d'applications qui sont autorisées à s'exécuter sur les systèmes de votre organisation. Une liste d'applications autorisées est un moyen efficace d'empêcher les programmes malveillants et non autorisés de s'exécuter sur les systèmes organisationnels. Par ailleurs, l'application fréquente des correctifs et des mises à jour aux systèmes d'exploitation et aux applications offre à votre organisation une couche de sécurité supplémentaire. Pour de plus amples renseignements à ce sujet, veuillez consulter l'ITSM.10.096, *Les 10 mesures de sécurité des TI : Nº 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications* [5]. Ce document offre des pratiques exemplaires sur la gestion des mises à jour et des correctifs pour vos systèmes d'exploitation et vos applications.

4 Contenu complémentaire

4.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Expression au long
AC	Contrôle d'accès (*Access control*) (code de la famille de contrôles de sécurité)
GIA	Gestion de l'identité et de l'accès
MV	Machine virtuelle
PIZ	Point d'interface de zone
RBAC	Contrôle d'accès basé sur les rôles (*Role-based access control*)
SC	Protection des systèmes et des communications (*System and communications protection*) (code de la famille de contrôles de sécurité)
SE	Système d'exploitation
SQL	Langage de requête structuré (*Structured query language*)
TI	Technologies de l'information
XSS	Script intersites (*Cross-site scripting*)
ZG	Zone de gestion

4.2 Glossaire

Terme	Définition
Application Web	Tout programme auquel on peut accéder au moyen d'une connexion réseau et qui utilise des technologies et navigateurs Web pour exécuter des tâches sur Internet, notamment les services de courrier, les logiciels de traitement de texte, les convertisseurs de fichiers, les solutions de commerce électronique et les calendriers.
Bac à sable	Espace virtuel dans lequel un logiciel nouveau ou non testé peut s'exécuter de façon sécurisée et son comportement peut être observé avant de l'autoriser sur un domaine ou un système.
Bien de TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
Confidentialité	Valeur qui est accordée à un ensemble d'information pour indiquer son niveau de sensibilité et les restrictions d'accès mises en place pour empêcher les utilisateurs non autorisés d'y accéder.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des biens de TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des stratégies, des pratiques et des procédures de sécurité.
Contrôle de sécurité de gestion	Classe de contrôles de sécurité qui porte principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.

Terme	Définition
Contrôle de sécurité opérationnel	Classe de contrôles de sécurité qui est principalement mise en œuvre et exécutée par des personnes, mais habituellement fondée sur l'utilisation de la technologie, par exemple, un logiciel de soutien.
Contrôle de sécurité technique	Classe de contrôles de sécurité qui est mise en œuvre et exécutée par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité intégrés aux composants matériels, logiciels et micrologiciels.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à infiltrer un système informatique, un réseau ou un dispositif.
Déni de service	Toute activité qui rend un système inaccessible aux utilisateurs légitimes ou qui provoque des retards dans les opérations et les fonctions du système.
Disponibilité	Valeur qui est accordée aux biens d'information, aux logiciels et au matériel (l'infrastructure et ses composantes). Les données ayant la cote de disponibilité la plus élevée doivent être accessibles en permanence. Il est également entendu que la disponibilité comprend la protection des biens contre les accès non autorisés et les compromissions.
Injection SQL	Méthode d'attaque employée par les auteures et auteurs de menace qui consiste à profiter des défauts de conception en matière de sécurité dans les formulaires Web pour injecter du code malveillant ou du code utilisé à des fins malveillantes.
Intégrité	Valeur qui est accordée à l'information pour indiquer dans quelle mesure elle est susceptible à la perte de données. Il est également entendu que l'intégrité comprend l'aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Liste d'applications autorisées	Liste des applications et des composants d'applications (p. ex. programmes exécutables, bibliothèques de logiciels, fichiers de configuration) dont l'installation et l'exécution sont autorisées sur des systèmes organisationnels.
Machine virtuelle	Ordinateur avec système d'exploitation pouvant exécuté des applications, mais qui n'existe pas physiquement. Il s'agit de l'équivalent émulé d'un système informatique.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice à l'information et aux biens de TI.
Mise en conteneur	Isolation complète d'une technologie par rapport à une autre.
Risque	Degré de probabilité qu'un auteur ou auteure de menace exploite une vulnérabilité pour accéder à un bien, et répercussions connexes.
Script intersites	Méthode d'attaque employée par les auteures et auteurs de menace qui consiste à profiter des lacunes en matière de sécurité pour injecter des scripts malveillants dans une application Web bénigne et de confiance.
Virtualisation	Technologie pouvant être utilisée pour créer des environnements simulés ou des ressources virtuelles (p. ex. serveur, poste de travail, système d'exploitation, stockage, réseau).
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée par un auteur de menace en vue de compromettre les biens ou les activités d'une organisation.

4.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089), septembre 2021.
2	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), décembre 2014.
3	Open Web Application Security Project. OWASP Top 10 – 2021, mars 2021.
4	Centre canadien pour la cybersécurité. Les 10 mesures de sécurité des TI : Nº 10, Mettre en place une liste d'applications autorisées (ITSM.10.095), août 2022.
5	Centre canadien pour la cybersécurité. Les 10 mesures de sécurité des TI : Nº 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications (ITSM.10.096), août 2022.

Annexe A Catalogue des contrôles de sécurité de l'ITSG-33

A.1 Contrôle de sécurité technique : contrôle d'accès

Le tableau 2 décrit le contrôle **AC-6 Droit d'accès minimal**, tel qu'il est défini à l'annexe 3A de l'ITSG-33 [2].

Tableau 2 : Contrôle de sécurité technique de l'ITSG-33 : AC-6 Droit d'accès minimal

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
AC-6	Droit d'accès minimal	(A) L'organisation utilise le principe du droit d'accès minimal, ce qui autorise l'accès uniquement aux utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées conformément aux missions et aux fonctions opérationnelles de l'organisation.	**Domaines de traitement séparés :** Le système d'information fournit des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès utilisateur. Voir les contrôles connexes AC-4, SC-3, SC-30 et SC-32.	AC-2 AC-3 AC-5 CM-6 CM-7 PL-2

A.2 Contrôle de sécurité technique : protection des systèmes et des communications

Le tableau 3 décrit le contrôle **SC-32 Partitionnement des systèmes d'information**, tel qu'il est défini à l'annexe 3A de l'ITSG-33 [2].

Tableau 3 : Contrôle de sécurité technique de l'ITSG-33 : SC-32 Partitionnement des systèmes d'information

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SC-32	Partitionnement des systèmes d'information	(A) L'organisation partitionne le système d'information en [composants de systèmes d'information désignés par l'organisation] se trouvant dans des domaines ou environnements physiques distincts en fonction de [circonstances propices à la séparation physique des composants définies par l'organisation].	Aucune	AC-4 SA-8 SC-3 SC-7