Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Approche à vérification systématique pour l'architecture de sécurité

Gestion

ITSM.10.008

Canada

Avant-propos

Approche à vérification systématique pour l'architecture de sécurité (ITSM.10.008) est une publication NON CLASSIFIÉ publiée par le Dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, prière d'envoyer un courriel ou de téléphoner au Centre de coordination des services du Centre pour la cybersécurité :

Centre de coordination des services

contact@cyber.gc.ca

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

Date d'entrée en vigueur

Cette publication entre en vigueur à compter du 15 mars 2023

Historique des révisions

Version	Modifications	Date
1	Première publication.	15 mars 2023

ISBN 978-0-660-48190-6
CAT D97-4/10-008-2023F-PDF

Vue d'ensemble

Cette publication offre une description des concepts associés à l'approche à vérification systématique (ZT en anglais pour « zero trust ») et de l'information sur comment les organisations peuvent tirer avantage de la mise en œuvre d'un modèle à vérification systématique (MVS) afin de protéger leurs actifs. Elle permettra d'aider les organisations à comprendre l'importance de migrer vers une architecture de sécurité à vérification systématique. En particulier, nous soulignerons l'importance des changements de façons de penser et de l'implication de tous les membres de l'organisation pour améliorer la posture de cybersécurité de l'entreprise. Nous décrirons des concepts associés à un MVS et fournirons de l'information sur comment les organisations peuvent tirer avantage de la mise en œuvre d'un MVS. De plus, nous présenterons quelques pratiques exemplaires que les organisations peuvent adopter pour la priorisation des efforts lors de la mise en œuvre d'une architecture à vérification systématique (AVS).

Sélectionner les lignes directrices ou le cadre général et trouver des experts et des ressources de confiance sont des étapes importantes de la mise en œuvre et de l'amélioration continue d'une approche à vérification systématique efficace.

Le gouvernement du Canada (GC) travaille à mettre au point un cadre de sécurité à vérification systématique qui aidera les services et les agences du GC à améliorer leur posture de sécurité générale. Le cadre de sécurité à vérification systématique du GC sera aligné aux piliers de la CISA et aux lignes directrices du NIST. En attendant, afin d'aider les organisations à sélectionner un cadre ou des lignes directrices alignés à leurs exigences d'affaires et à leur infrastructure réseau, nous présentons un aperçu de trois cadres ou système de lignes directrices de confiance ayant trait à un MVS :

- National Institute of Standards and Technology (NIST) : special publication 800-207: Zero Trust Architecture [1]
- Cybersecurity and Infrastructure Security Agency (CISA) : Zero Trust Maturity Model [2]
- National Cyber Security Center (NCSC) : Zero trust architecture design principles [3]

Table des matières

Liste des figures

Liste des tableaux

1 Introduction

Les réseaux informatiques connaissent une croissance en taille et en complexité afin de répondre aux exigences d'affaires. De plus, ils intègrent de nouvelles technologies en pleine évolution, comme les infrastructures en nuage hybrides. Les cybermenaces se sont adaptées aux changements et tirent souvent avantage des lacunes de sécurité qui découlent des transformations précipitées. Les utilisateurs, les données et les services sont désormais dispersés sur plusieurs emplacements et il n'y a plus de périmètre défini entourant les ressources organisationnelles. Les organisations ne peuvent plus se fier aux techniques de défense traditionnelles basées sur le périmètre pour protéger les systèmes critiques, et c'est pourquoi les approches à vérification systématique sont plus importante que jamais.

1.1 Qu'est-ce qu'une architecture à vérification systématique et un modèle à vérification systématique?

Une AVS est une approche d'entreprise de conception de système où les perspectives de sécurité sont basées sur les principes d'un MVS. Le principe de base est qu'il n'est jamais possible d'établir une confiance inhérente par défaut pour un sujet.

Au sein d'une AVS :

- chaque interaction établie entre un utilisateur et une ressource nécessite des mécanismes d'authentification et d'autorisation renforcés
- la granularité du contrôle d'accès aux ressources est aussi précise que possible
- les décisions de contrôle d'accès sont basées sur une **évaluation dynamique** du contexte de confiance pour chaque demande d'accès

Dans le cadre d'une approche à vérification systématique, les communications entre les utilisateurs, les systèmes et les appareils sont authentifiées, autorisées et validées en continu. Ces opérations reposent sur des contrôles d'accès basés sur les politiques (PBAC), comme le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basés sur les privilèges (ABAC). Une AVS applique les politiques d'accès en fonction du contexte, tenant compte par exemple du rôle de l'utilisateur, du moment de la journée, de la géolocalisation, de l'appareil et des données demandées. Le niveau d'accès accordé est ajusté dynamiquement selon le niveau de confiance du sujet établi. En bref, plus la confiance établie par le système informationnel envers le sujet est grande, plus le niveau d'accès du sujet peut être élevé.

Une AVS préviendra également les mouvements horizontaux au sein de l'environnement des TI. Il est important de noter que la prévention des mouvements horizontaux est l'objectif premier d'un MVS, et non l'élimination des défenses de périmètre héritées ou des appareils PAP (prenez vos appareils personnels). Ces points peuvent être intégrés à un MVS, mais ils ne devraient pas s'agir du motif principal de sa mise en œuvre.

Selon le NIST [1], les définitions pratiques de MVS et d'AVS correspondent à ce qui suit :

> Un modèle à vérification systématique (MVS) fournit une collection de concepts et d'idées visant à réduire l'incertitude liée à l'application de décisions précises d'accès pour chaque demande en fonction du principe de droit d'accès minimal
> aux systèmes d'information et aux services dans un réseau considéré comme étant compromis. Une architecture à

vérification systématique (AVS) est un plan de cybersécurité d'entreprise exploitant les concepts et les composants connexes d'un MVS ayant trait aux relations, à la planification des flux de travaux et aux politiques d'accès. Ainsi, une entreprise qui adopte les principes d'un MVS présente une infrastructure réseau (physique et virtuelle) et des politiques opérationnelles en place afin de planifier une AVS.

On recommande aux organisations de mettre en œuvre les principes de MVS de manière incrémentielle et d'utiliser, si possible, une approche à vérification systématique hybride intégrant le modèle de protection basé sur le périmètre jusqu'à une transition complète vers le MVS. Cela devrait être fait tout en continuant d'investir dans des initiatives de modernisation de la sécurité pour améliorer la posture de cybersécurité de l'organisation. Un MVS utilisé conjointement à une approche basée sur le risque pour la gestion des risques liés à la sécurité, comme la gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [4], favorisera la flexibilité, l'agilité et l'adaptabilité des organisations, tout en assurant la sécurité, la confidentialité, l'intégrité et la disponibilité des actifs de l'entreprise.

1.2 Approche de sécurité à vérification systématique

La migration vers un MVS est un processus complexe qui peut nécessiter d'apporter des changements à tous les niveaux organisationnels. Les dirigeants, les administrateurs et les intervenants des organisations, ainsi que les utilisateurs, doivent collaborer pleinement dans la mise en œuvre des nouvelles technologies, des pratiques de travail et des politiques afin d'améliorer la protection et de soutenir la mise en place d'une AVS. Grâce à un MVS, vous pouvez améliorer la posture de sécurité de votre organisation tout en améliorant l'utilisation des ressources, la conformité et la résilience à tous les niveaux. Un changement d'état d'esprit est toutefois nécessaire pour l'adoption d'une approche à vérification systématique. En particulier, vous devez adopter les perspectives suivantes :

- les connexions à votre infrastructure réseau et aux ressources sont toutes potentiellement hostiles
- le trafic réseau et les demandes d'accès à vos ressources peuvent être malveillants
- les auteurs de menace tenteront une écoute clandestine des communications et des flux de données
- l'intégration de la journalisation et de la surveillance des demandes d'accès, des activités de gestion du système, des changements de configuration et du trafic réseau doit faire partie de votre mise en œuvre afin de mesurer l'intégrité et la posture de sécurité de tous les actifs
- l'authentification, la vérification explicite et l'autorisation de chaque demande d'accès doivent respecter le principe de droit d'accès minimal, et les demandes d'accès en question doivent avoir une durée de vie déterminée
- les décisions de contrôle d'accès doivent reposer sur des politiques dynamiques basées sur les risques
- tout accès accordé à des ressources sensibles augmente votre risque vis-à-vis des cybermenaces
- la mise au point d'une intervention en cas d'incident et d'un plan de reprise limitera des dégâts et assurera la continuité des activités.

2 Cadres MVS acceptés dans l'industrie

Les agences et les organisations fédérales ont tendance à ne plus se fier uniquement aux mécanismes de sécurité ayant trait à la défense du périmètre et adoptent de plus en plus une approche à vérification systématique. Pour ce faire, nous les encourageons à consulter les cadres et les lignes directrices de MVS de confiance. La CISA, le NIST et le NCSC ont publié des lignes directrices d'une approche à vérification systématique afin d'aider les agences et les organisations à mettre au point et à mettre en œuvre un cadre de MVS. Ainsi, les agences et les organisations pourront personnaliser leur MVS en fonction des besoins liés à leurs activités, de leur mission et du contexte de menace qui s'applique.

La présente section offre une brève description des cadres MVS acceptés dans l'industrie. Pour une présentation plus détaillée, consultez le document.

Le **GC** travaille à l'élaboration d'un cadre de sécurité à vérification systématique qui sera aligné aux piliers de la CISA et du NIST. L'objectif du GC pour le passage à un MVS est le suivant :

- continuer d'offrir un écosystème de sécurité numérique d'entreprise résilient assurant une prestation des services du gouvernement en toute sécurité
- fournir une expérience utilisateur transparente et améliorée pour les utilisateurs autorisés
- fournir une plateforme sécuritaire assurant la protection des systèmes et des données hébergées
- (physiques et virtuelles) dans l'environnement en réseau convergé du GC
- offrir une protection de bout en bout de l'information, des applications, des appareils, des réseaux, du matériel et des installations physiques du GC
- mettre au point, adopter et appliquer des processus, une structure de gouvernance et des normes matures ayant trait à la sécurité
- assurer la confidentialité, l'intégrité et la disponibilité de l'infrastructure des technologies de l'information (TI) du GC, des données critiques des clients et des données critiques relatives aux activités du GC

En attendant la publication du cadre de MVS du GC, on encourage les organisations à s'inspirer des cadres de sécurité couramment utilisés et à appliquer les lignes directrices du NIST, de la CISA ou du NCSC. Sélectionner un cadre MVS et respecter les lignes directrices des ressources de confiance sont des étapes importantes pour la mise en œuvre d'une stratégie efficace.

Le **NIST** a mis au point les lignes directrices d'une approche à vérification systématique pour concevoir et déployer une AVS et suggère d'adhérer à sept principes généraux, que nous détaillerons dans la présente section.

Les lignes directrices du **Department of Defense (DoD) et de la National Security Agency (NSA)** présentent une approche à vérification systématique plus axée sur les niveaux opérationnels et les microniveaux que celles du NIST. L'AVS de la NSA est très similaire à celle de la DoD et présente les sept mêmes principes de base. L'objectif des deux architectures est toutefois différent. L'AVS de la DoD a été mise au point en tenant compte de la mission et des exigences propres aux activités de défense et exploite le cadre d'architecture du Department of Defense (DoDAF). En contrepartie, l'AVS de la NSA a été mise au point pour les besoins de la NSA et des organisations de l'industrie de la défense.

La **CISA** a fait l'ébauche d'un modèle de maturité pour l'approche à vérification systématique inspiré des concepts de base des AVS de la DoD et de la NSA. Le MVS de la CISA est basé sur cinq piliers différents et appuyé par des capacités globales de visibilité, d'analyse, d'automatisation, d'orchestration et de gouvernance. Il a été créé pour aider tout type d'agence fédérale pour la mise au point d'une AVS.

Les lignes directrices du **NCSC (Royaume-Uni)** reposent sur huit principes, qui représentent les fondements et les considérations architecturales nécessaires pour mettre au point une AVS. Chaque organisation adoptera une approche à vérification systématique différente, en fonction de ses besoins opérationnels, des technologies utilisées et du contexte des menaces. Les lignes directrices du NCSC, qui tiennent compte de cette nécessité de personnalisation, considèrent néanmoins que la plupart des approches doivent adopter les huit principes de base en question.

3 Avantages de l'utilisation d'un cadre de sécurité MVS

Un cadre de sécurité à vérification systématique est une approche globale visant à améliorer la posture de sécurité de votre organisation et à protéger les données et les actifs numériques sensibles.

Il existe plusieurs avantages de mettre en œuvre une AVS au sein de votre organisation. En voici quelques-uns :

1. **Offre une meilleure protection réseau et contre les mouvements horizontaux**

   Nous entendons souvent parler d'attaques faites à partir d'un compte d'utilisateur compromis ou d'un appareil utilisé à titre de point d'entrée dans le réseau d'une organisation. Lorsque la plupart des contrôles de sécurité sont à l'intérieur du périmètre réseau de l'organisation, il est difficile de détecter un assaillant ayant percé la première couche de défense. Une fois entré, l'assaillant progressera de façon horizontale dans le réseau afin d'accéder aux justificatifs d'identité ou à d'autres informations sensibles. Dans une approche à vérification systématique, les applications et les services ne peuvent communiquer qu'après leur authentification. Un MVS réduit le risque d'un mouvement horizontal, car toutes les communications, peu importe l'origine, sont considérées comme non fiables et nécessitent l'obtention d'un accès particulier.

   Dans un MVS, toutes les actions des utilisateurs ou des appareils sont soumises à une certaine forme de décision liée aux politiques. Cela permet à l'organisation de vérifier chaque tentative d'accès aux données ou aux ressources. Ainsi, il est plus difficile pour un assaillant de pénétrer dans le système.

2. **Offre une meilleure visibilité et une surveillance améliorée**

   Une approche à vérification systématique exige que les organisations consignent tous les appareils accédant à l'information ou aux ressources du réseau et en assurent la conformité. Elle exige aussi que chaque utilisateur soit soumis à un processus d'authentification rigoureux afin d'obtenir accès à des ressources particulières. Cela offre plus de visibilité à propos des personnes qui accèdent aux ressources, et à quelle fin. Il est ainsi plus facile de déterminer les mesures de sécurité devant être appliquées à chaque ressource. Un MVS nécessite une surveillance continue de toutes les activités et communications. Les organisations bénéficient de la sorte d'une visibilité complète du trafic de leur réseau. Elles peuvent mieux détecter les menaces potentielles et assurer une réponse rapide.

3. **Améliore la détection des incidents et la réponse à ceux-ci**

   Un MVS offre de nouvelles capacités d'intervention en cas d'incident grâce à de l'information détaillée à propos des demandes d'accès suspectes, de l'utilisateur, de l'appareil, des données et de l'application impliqués. Par conséquent, lorsqu'un incident est découvert, il peut être associé à des entités, à des applications et à des données précises.

4. **Améliore le contrôle de l'accès au nuage**

   Le contrôle de l'accès et la visibilité sont les plus grandes préoccupations des organisations lors de leur migration vers le nuage. Bien que les fournisseurs de services infonuagiques (FSI) offrent certaines fonctionnalités de sécurité, la responsabilité de la protection des actifs de votre organisation est partagée entre vous et le FSI. Vous disposez d'un contrôle limité à l'intérieur du nuage.

Un MVS nécessite que tous les actifs du nuage soient catégorisés de manière à leur appliquer des caractéristiques de protection et de contrôle d'accès. Dans le cadre d'un MVS, vous pouvez vous assurer que toute tentative de connexion à votre infrastructure infonuagique est légitime.

5. **Améliore la protection des données**

Traditionnellement, en cas d'intrusion de votre périmètre réseau (par exemple à partir d'un coupe-feu), l'assaillant peut exploiter un mouvement horizontal afin de potentiellement trouver et voler de l'information sensible, des données de client ou une propriété intellectuelle. Cela peut causer des dommages à la réputation de votre organisation et potentiellement avoir des répercussions juridiques. En passant d'une défense axée sur le périmètre à une approche visant à sécuriser les ressources individuelles, les organisations réduisent le risque de violation et de vol de données.

Une authentification robuste et la validation des connexions en fonction des principes d'un MVS permettent d'assurer le respect de la confidentialité. Un MVS adopte le principe de droit d'accès minimal et accorde un accès aux utilisateurs seulement pour leur permettre de réaliser leurs tâches. Pour chaque demande de connexion, l'entité est présupposée hostile tant que l'utilisateur et l'appareil ne sont pas authentifiés et que les autorisations ne sont pas accordées. L'accès est continuellement revérifié, en fonction des changements d'état, comme l'emplacement de l'utilisateur et le type de données demandé.

6. **Favorise une conformité continue et facilite les activités de vérification**

Une AVS favorise aussi la conformité continue des normes et des réglementations ayant trait à la confidentialité en évaluant et en journalisant chaque demande d'accès. Ainsi, le suivi de l'identité de l'utilisateur et de l'application, avec des données temporelles et de localisation au moment de la demande, permettent une piste de vérification complète. De la sorte, un effort minimal est nécessaire pour répondre aux exigences de vérification et assurer la gouvernance.

7. **Assure la sécurité des effectifs à distance**

Un défi important des organisations actuelles est d'offrir un écosystème de travail à distance. Les utilisateurs travaillent de la maison, et les données sont partagées. De la sorte, les modèles de défense de périmètre, comme le recours à des coupe-feu, ne sont plus suffisants. Tout employé distant ou hybride augmente la surface d'attaque et crée de nouvelles possibilités d'entrée pour les assaillants. Dans un MVS, la segmentation du réseau et la création de micropérimètres, avec des politiques d'identification et de validation rigoureuses, le contrôle est fourni à un utilisateur précis utilisant un appareil et une application et se trouvant dans une zone sécurisée.

4 Pratiques exemplaires pour la mise en œuvre d'une AVS

Dans la présente section, nous décrirons quelques pratiques exemplaires à suivre pour vous aider à mettre en œuvre l'AVS de votre organisation.

1. **Authentification de toutes les connexions**

   Vous ne devez jamais faire confiance à votre réseau local. Dans les architectures traditionnelles, on fait confiance à toute connexion réseau provenant du périmètre intérieur. On suppose que l'utilisateur ou l'activité du réseau a déjà été authentifié et autorisé. Plutôt que de faire confiance implicitement aux connexions réseau qui proviennent logiquement de votre réseau local, toutes les connexions doivent être authentifiées adéquatement. Au minimum, il est nécessaire d'authentifier l'utilisateur ainsi que l'appareil de la demande d'accès avant d'établir une connexion. Lorsque des mesures de sécurité plus rigoureuses sont nécessaires, il est possible d'ajouter la géolocalisation, la date et l'heure aux exigences d'authentification. Dans le cadre d'un MVS, vous devez établir la confiance envers les appareils, les utilisateurs et les services associés à votre réseau.

2. **Mise en œuvre de politiques à vérification systématique**

   La création et la mise en œuvre de politiques sont les étapes les plus importantes, et les plus exigeantes, du point de vue de la main-d'œuvre, nécessaires pour établir une AVS robuste. Les organisations doivent réellement comprendre tous les aspects de la protection et des niveaux nécessaires pour la sécurisation des flux de données.

   Lors de la mise au point et de la mise en œuvre de politiques d'un MVS, posez-vous les questions suivantes :

   - Qui sont les utilisateurs?
   - Qu'est-ce qu'ils doivent accéder?
   - Pourquoi doivent-ils avoir accès à ces ressources?
   - À partir d'où les accès seront demandés?
   - Où se trouvent les utilisateurs et les points d'extrémité des demandes d'accès?
   - Comment accorder et approuver les accès?

3. **Création d'un « moteur de confiance »**

   Un moteur de confiance sert à évaluer la confiance, et par la suite à permettre ou à refuser l'accès selon la collecte et l'évaluation d'une grande quantité d'attributs pertinents au contexte de sécurité de la demande d'accès. Voici quelques éléments potentiels à considérer :

   - état de sécurité des appareils associés à la demande (versions logicielles, correctifs appliqués, emplacement physique et logique, date et heure, statut de surveillance, historique d'accès observé, etc.)
   - attributs comportementaux du demandeur (motifs d'utilisation, moment de la journée, etc.)
   - attributs au niveau de l'entreprise qui représentent le contexte de sécurité actuel (par exemple, état de sécurité rehaussé en fonction de la surveillance et d'indicateurs d'événement)

Le cœur d'un MVS est l'établissement d'un « moteur de confiance » dynamique ayant une visibilité globale à tous les niveaux de l'architecture et qui intègre les flux des composants clés pour la sécurité opérationnelle. La mise au point de ce moteur de confiance nécessitera d'y consacrer du temps et des efforts.

4. **Connaissance des actifs et de l'architecture du réseau**

Lors de la création d'une AVS, il est important de connaître vos actifs et votre architecture de réseau. Créez un inventaire de vos données, de vos utilisateurs, de vos appareils et de vos applications pour l'accès de votre réseau. Vous devez savoir comment contrôler et gérer les demandes d'accès et les compromissions potentielles pouvant survenir si l'accès est accordé. Vous devez également savoir la valeur des données de votre organisation et les risques d'une compromission potentielle des données. Cela est essentiel pour appliquer tout changement d'importance à votre architecture et à votre environnement informatique.

5. **Utilisation de l'authentification multifacteur (AMF)**

Avec l'AMF, deux ou plusieurs facteurs d'authentification sont nécessaires pour déverrouiller un appareil ou pour se connecter à un compte. L'AMF utilise une combinaison des facteurs suivants pour authentifier un utilisateur : quelque chose que vous avez, quelque chose que vous connaissez ou quelque chose qui vous caractérise. Ces facteurs peuvent et doivent être ajustés, en fonction de la sensibilité des données et des ressources à accéder. L'AMF réduit significativement les possibilités qu'un assaillant puisse utiliser des justificatifs d'identité compromis afin d'accéder à vos systèmes et à vos données. Cela est un préalable essentiel pour une approche à vérification systématique.

Pour mieux comprendre comment l'AMF peut aider à sécuriser vos appareils et vos comptes, consultez le document Sécurisez vos comptes et vos appareils avec une authentification multifacteur [5]. Si vous avez besoin d'aide pour déterminer le niveau cible de l'assurance de l'authentification, vous pouvez consulter notre guide technique Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information [6]. Celui-ci complète celui du Secrétariat du Conseil du Trésor (SCT) Ligne directrice sur la définition des exigences en matière d'authentification [7].

6. **Utilisation du chiffrement pour tout le trafic**

Une approche à vérification systématique exige le chiffrement de tout le trafic pour l'application du pilier ayant trait à accorder un accès explicite aux ressources. Cela est contraire au modèle de défense de périmètre traditionnel où l'accès est fourni de manière intrinsèque. Le chiffrement contribue à la prévention de la perte de données, car les fichiers fuités ou volés sont inutilisables sans un déchiffrement. Pour la même raison, le chiffrement aide à protéger l'information de bout en bout et à protéger contre le reniflage des données.

7. **Accès en fonction des politiques**

Les organisations doivent mettre au point des politiques dynamiques basées sur risque et s'assurer que celles-ci sont appliquées correctement. Ces politiques présentent un ensemble de règles d'accès liées aux utilisateurs, aux données, aux actifs, aux applications et aux services. Les politiques d'autorisation d'accès aux ressources pourront

varier en fonction de leur sensibilité. Le principe de droit d'accès minimal doit être appliqué afin de restreindre à la fois la visibilité et l'accessibilité.

Avec une approche à vérification systématique, la confiance implicite associée à l'emplacement réseau (adresse IP) n'est plus une condition d'authentification. À la place, une authentification basée sur l'identité sert à établir la confiance et à accorder l'accès à des ressources particulières, à un moment donné et à partir d'un emplacement ou d'un appareil spécifique.

8. **Utilisation d'une gestion des accès privilégiés (PAM) et de postes de travail administratifs sécurisés (SAW)**

La gestion des accès privilégiés sert à protéger tous les comptes d'administrateur qui nécessitent des privilèges supérieurs. Lorsqu'un accès administratif de haut niveau est requis, celui-ci doit être accordé selon le principe d'accès juste-à-temps. Il s'agit d'un accès temporaire qui est révoqué dès que la tâche est terminée et que l'accès n'est plus nécessaire. Avant d'accorder à toute personne une session à accès privilégié, la demande de la session doit avoir été vérifiée et acceptée par un utilisateur différent. Cela prévient qu'une personne s'accorde à elle-même un accès privilégié sans les approbations nécessaires.

Des solutions PAM peuvent automatiser ce processus d'approbation ainsi qu'enregistrer tout ce qui a été réalisé dans la session avec accès privilégié.

Un poste de travail administratif sécurisé, qui est une machine physique ou virtuelle consacrée à cette fonction, ne doit servir aux administrateurs que pour réaliser des tâches administratives. Ce poste de travail sécurisé répond aux exigences de sécurité pour les administrateurs des TI travaillant avec des serveurs et des applications afin de mener des tâches sensibles associées à un risque élevé en cas de compromission. Un poste de travail dédié ne peut pas servir pour la navigation sur le Web, le courriel ou d'autres applications à risque.

La solution PAM est étroitement liée au poste de travail administratif sécurisé. Les utilisateurs doivent se connecter au poste de travail administratif sécurisé au moyen de la solution PAM pour accéder à des comptes protégés. Une plateforme PAM peut être utilisée pour sécuriser et contrôler tous les accès aux comptes à accès privilégié, y compris les accès privilégiés individualisés, le moment d'accès affecté et les actions permises.

9. **Mise en œuvre du principe de droit d'accès minimal, du contrôle d'accès basé sur les rôles (RBAC) et du contrôle d'accès basés sur les privilèges (ABAC)**

Dans un MVS, il est important d'appliquer le principe de droit d'accès minimal partout où cela est possible, en particulier pour les accès privilégiés et la gestion de la sécurité. Un MVS repose sur le principe qu'un utilisateur ne doit avoir accès qu'à ce qui lui est nécessaire pour accomplir une tâche particulière. Un RBAC peut être mis en œuvre pour renforcer le principe de droit d'accès minimal de façon codifiée, où les droits d'accès des utilisateurs sont mis en correspondance avec leur rôle dans l'organisation. La combinaison d'un RBAC à une solution PAM améliorera davantage le contrôle d'accès au sein de votre organisation.

Grâce à un ABAC, les privilèges d'accès ont une granularité très fine; ils sont définis afin de déterminer quels sont les utilisateurs ayant accès aux données particulières. Dans le cas d'un ABAC, les politiques de contrôle d'accès sont basées sur des règles, en fonction des caractéristiques et des propriétés de chaque demandeur. Chaque point

de données est vérifié afin d'assurer que les attributs correspondent aux données d'autorisation du demandeur, avant d'accorder un accès.

10. **Surveillance et journalisation des appareils et des accès aux services**

Il est important de surveiller en continu comment les appareils et les services interagissent, ce qui est demandé, les activités réalisées et quelles sont les données en jeu. Une journalisation continue des données et l'utilisation d'une analyse de sécurité pour signaler les anomalies à étudier aideront à identifier les activités suspectes ou à détecter et à freiner les attaques. Une solution de gestion des informations et des événements de sécurité (GIES) facilitera et accélérera la collecte, la mise en corrélation et les analyses de grandes quantités de données pour les administrateurs. Une GIES peut offrir le niveau de visibilité nécessaire pour s'assurer que tous les utilisateurs connectés au réseau sont dignes de confiance, une partie essentielle d'une approche à vérification systématique.

11. **Gestion de tous les appareils**

La vérification de vos utilisateurs est nécessaire, mais non suffisante. Les principes d'un MVC s'appliquent également aux points d'extrémité. Pour vérifier que seuls les appareils de confiance sont connectés à votre réseau, associez un identificateur unique à chacun et intégrez des activités de traçabilité. Un identificateur offre plus de visibilité sur votre réseau et exposera les appareils non autorisés. L'identificateur associé aux appareils sera nécessaire pour accorder les autorisations et les accès et pour les politiques que vous définissez. Les politiques ainsi définies doivent intégrer la certification d'appareil, la configuration et la conformité. Les certifications d'appareil peuvent aider au contrôle de l'inventaire ainsi que pour l'authentification. Elles doivent être chiffrées et protégées par un mot de passe. Ainsi, en cas de fuite, elles seront tout de même difficiles à exploiter.

Le système d'exploitation et les applications exécutés sur l'appareil doivent être configurés correctement, avec un provisionnement sécurisé et à jour. Un système de contrôle d'accès doit être en place pour assurer l'application des contrôles de politique, avant l'accès à l'information ou aux données. L'accès doit être modifié si une fonctionnalité de sécurité n'est pas au niveau de conformité requis.

L'utilisation d'un module de plateforme de confiance (TPM) peut s'avérer très utile pour ce faire. Un TMP est un circuit intégré (CI) servant à la sécurité cryptographique. Il s'agit d'une approche matérielle pour l'authentification d'un appareil. Il stocke de manière sécurisée les artéfacts, comme les mots de passe, les certificats et les clés de chiffrement pour la gestion de l'authentification des appareils et des utilisateurs, les accès au réseau et la protection des données. On retrouve des TPM dans les ordinateurs personnels (PC), les carnets électroniques, les téléphones mobiles et l'équipement réseau.

Les effectifs modernes exploitent couramment les politiques PAP et utilisent des appareils mobiles dans le contexte professionnel. Dans le cadre d'un MVS, tous les appareils doivent être authentifiés individuellement avant d'accorder un accès aux ressources et aux données de l'organisation. Cela offre un meilleur contrôle pour les environnements PAP. Les administrateurs des TI peuvent ainsi établir et appliquer des politiques très précises pour l'autorisation et l'authentification en déterminant les caractéristiques nécessaires d'un appareil pour accéder aux ressources.

12. **Utilisation d'une segmentation ou d'une microsegmentation du réseau**

La segmentation de réseau est une des approches potentielles pouvant être utilisées lors de la mise en œuvre d'un AVS. Il s'agit de la pratique visant à créer des sous-réseaux au sein du réseau général afin d'empêcher les assaillants de se déplacer latéralement une fois à l'intérieur du périmètre. Normalement, les entreprises établissent des segments de réseau au moyen de réseaux locaux virtuels (VLAN) accompagnés de coupe-feu, de sous-réseaux, et de zones de sécurité.

Une microsegmentation divise logiquement les environnements de centre de donnée et infonuagiques en segments de sécurité distincts, pouvant aller jusqu'au niveau de la personne. Une telle segmentation dépend fortement de l'utilisation de points d'application de politique au sein du réseau afin de contrôler dynamiquement les communications entre les composants, en fonction de la politique. Cela sert à protéger les données et les services sensibles des menaces internes et externes. La microsegmentation offre une sécurité multicouche et permet de restreindre les accès aux actifs à un niveau très précis. Ainsi, même si un assaillant pénètre dans votre réseau, les dommages seront limités.

13. **Utilisation d'un périmètre défini par le logiciel (SDP)**

Un périmètre défini par le logiciel peut soutenir plusieurs concepts et principes d'un MVS. Cela comprend un contrôle d'accès très précis en fonction du principe de droit d'accès minimal pour toutes les demandes d'accès, un chiffrement des données en transit, une microsegmentation, etc. Il s'agit d'une solution de rechange aux réseaux privés virtuels (RVP) et offre un accès à distance sécurisé à toute application, peu importe l'emplacement. Un SDP correspond à un réseau doté de frontières logicielles, et non matérielles. Les SDP reposent sur un modèle de confiance adaptatif où l'accès est accordé en fonction des identificateurs d'utilisateur et du principe de droit d'accès minimal. Ils sont définis par les politiques et principes du MVS, et non l'adresse IP. Ainsi, les utilisateurs distants peuvent se connecter à une application sans avoir un accès au réseau. La surface d'attaque est de la sorte réduite.

5 Défis pour les organisations

Les organisations devront surmonter de nombreux défis lors de la transition vers un MVS. Avec un tel modèle, les activités d'authentification d'accès, de vérification et de suivi doivent être contrôlées à un niveau très précis, et de nombreuses technologies plus anciennes ne sont pas compatibles avec cela. Les organisations devront également avoir une compréhension globale de leurs exigences d'affaires, ce qui est essentiel pour un MVS robuste. À titre de point de départ, les organisations devront réaliser ce qui suit :

- identifier les données, les actifs, les applications et les services critiques et précieux de leur réseau
- savoir qui sont les utilisateurs, les applications et les services qu'ils utilisent, leur géolocalisation et la façon employée pour établir les connexions.

Cela permettra aux organisations de mieux concentrer leurs efforts pour prioriser et protéger les ressources dans le cadre de leur mise en œuvre d'un MVS. De plus, pour maintenir ou améliorer la posture de sécurité des organisations, on ajoutera une exigence ayant trait à la maturité de la sécurité et à l'intégration au sein de l'organisation et de toutes les couches technologiques. Les mécanismes de sécurité réseau traditionnels seront tout de même requis lors d'un passage à un MVS, puis après sa mise en œuvre, afin de soutenir la transition vers des zones de confiance plus précises. Ces mécanismes serviront également à titre de source d'information pour les moteurs de confiance de votre organisation.

Voici quelques exemples de défis que les organisations pourront avoir à relever :

- Les techniciens et les administrateurs de l'organisation devront améliorer leurs efforts pour définir et mettre en œuvre des privilèges d'accès pour chaque utilisateur et chaque ressource concernant les décisions de confiance et d'accès.
- Les utilisateurs pourront être contrariés d'avoir à utiliser l'authentification multifacteur (AMF) et à s'authentifier plus fréquemment au cours de leur travail.
- Les appareils devront obtenir des jetons d'authentification matériels, et un déploiement dans toute l'organisation peut être coûteux et exigeant en temps. Les coûts associés aux logiciels, au matériel et à la formation seront plus importants.
- Les coupe-feux plus anciens peuvent ne pas prendre en charge certaines des fonctionnalités dynamiques requises. Les plans en différentes phases pour l'insertion de nouvel équipement devront être équilibrés avec des considérations de coûts.
- Les ressources techniques pour la mise en œuvre d'un MVS peuvent être limitées.

Migrer vers une AVS peut apporter son lot d'instabilité, car la complexité de la période de transition dépend de la compatibilité ou non des systèmes avec un MVS. Le modèle de maturité de la CISA [2] présente un des nombreux parcours potentiels permettant de soutenir la transition vers un MVS. Ce modèle de maturité offre des exemples d'architectures traditionnelles, évoluées et optimales pour une AVS. Ainsi, les organisations pourront migrer vers une AVS de façon incrémentielle et, éventuellement, atteindre une posture de cybersécurité optimale.

Un changement permanent des mentalités devra être adopté et pleinement accepté pour le fonctionnement d'un MVS. La mise en œuvre d'un MVS nécessite des efforts globaux et intégrés. Si la solution ne bénéficie pas d'un soutien complet, y compris de la part de la direction, des administrateurs, des intervenants et des utilisateurs, cela peut ralentir les processus et affecter la productivité.

Plusieurs années peuvent être nécessaires pour l'adoption complète d'une AVS. Afin d'éviter les interruptions de productivité, on recommande que votre organisation adopte une mise en œuvre incrémentielle. Cela permettra une transition sans heurt et offrira plus de temps pour les ajustements nécessaires au nouveau cadre de sécurité, aux nouvelles politiques et aux nouveaux processus. Les organisations doivent savoir qu'un MVS ne représente pas une approche passive qui, après avoir été établie, reste inchangée. Il s'agit d'un investissement à long terme qui exige du temps, des efforts, des investissements financiers et une maintenance continue.

En fonction du rythme de croissance de vos activités, il est impératif que votre cadre MVS évolue en même temps que vous. Par exemple, les contrôles d'accès doivent être périodiquement mis à jour pour s'assurer que les bonnes personnes ont accès à de l'information particulière. Assurer la précision et la mise à jour des autorisations demande un entretien continu et il est impératif de bloquer les accès à l'information sensible.

Certains fournisseurs prétendront que leurs produits sont la réponse à l'adoption d'un MVS entièrement sécurisé. Méfiez-vous de telles déclarations. En réalité, il n'existe pas un fournisseur ou une solution à vérification systématique clé en main pour la mise en œuvre d'une AVS. Un MVS est plus qu'une solution technique et exige un changement fondamental dans la manière de gérer la sécurité.

6 Lignes directrices supplémentaires pour l'approche à vérification systématique

Dans l'environnement de menace actuel, où les cybermenaces sont de plus en plus sophistiquées, les organisations ne peuvent plus dépendre d'une défense basée sur le périmètre pour protéger les systèmes et les données critiques. Dans cette optique, le 12 mai 2021, la Maison blanche a émis le décret présidentiel 14028 sur l'amélioration de la sécurité nationale [8]. Celui-ci exigeait que le gouvernement fédéral des États-Unis agisse pour renforcer la cybersécurité nationale et réponde à un certain nombre d'objectifs de l'approche à vérification systématique d'ici la fin de l'année financière 2024. Le décret présidentiel présentait également la nécessité d'avoir « une surveillance de la sécurité complète; des contrôles d'accès basés sur le risque très précis; et une automatisation de la sécurité des systèmes de façon coordonnée pour tous les aspects de l'infrastructure dans le but de protéger les données en temps réel dans un environnement de menace dynamique ». Un plan de migration type évaluera l'état de cybersécurité actuel d'une agence et planifie une mise en œuvre complète d'AVS.

Les lignes directrices décrites dans la présente section offrent un point de départ pour l'utilisation d'un MVS afin de renforcer la sécurité. Elles s'appliquent à tous les aspects d'un environnement des TI. Toutes ces lignes directrices décrivent un MVS comme étant une approche de cybersécurité et répondent à la prémisse d'un MVS : ne jamais se fier, toujours vérifier. Il s'agit ainsi d'éliminer tous les cas de confiance implicite et de valider en continu toutes les étapes d'une interaction numérique.

6.1 Publication spéciale du NIST 800-207 : Zero Trust Architecture

Les lignes directrices du NIST en matière de MVS, dont la première publication remonte au mois d'août 2020, présentaient une liste des principes de base ayant trait à un MVS afin d'établir une AVS. Le principal objectif était d'aider les agences à réduire les zones de confiance implicite et à mieux comprendre l'infrastructure réseau et les communications des données, des applications et des systèmes informatiques. Les agences bénéficient ainsi d'un vaste bassin de cas d'utilisation où un MVS peut être mis en œuvre et où les principes des MVS peuvent être appliqués en fonction des directives de conformité fédérales.

Voici les sept principes de base recommandés par le NIST pour s'assurer de la réussite d'une approche à vérification systématique. Ces principes sont à la base d'une architecture qui répond aux principes d'un MVS.

1. **Chaque source de données et chaque service informatique est considéré comme étant une ressource**

   Tous les fichiers, toutes les données, tous les actifs numériques et tous les types de points d'extrémité contenant de l'information sur l'entreprise et qui communiquent au sein du réseau doivent être considérés comme étant des ressources.

2. **Toutes les communications doivent être sécurisées, peu importe l'emplacement sur le réseau**

   Dans un MVS, le réseau est toujours considéré comme étant hostile. Des contrôles de sécurité appropriés doivent être mis en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité des données en transit. Toutes les demandes d'accès aux actifs doivent répondre aux mêmes exigences de sécurité robustes d'authentification, peu importe d'où provient la demande. Les actifs peuvent se trouver dans l'infrastructure réseau détenue par l'entreprise

ou sur un réseau externe. Les mêmes normes de vérification de sécurité s'appliquent dans tous les cas. La confiance n'est jamais implicite.

3. **L'accès aux ressources individuelles de l'entreprise est accordé pour une session seulement**

   Dans une AVS idéale, l'accès à une ressource particulière (fichier, données, actif numérique) nécessite une authentification et une autorisation, avec une durée d'application limitée. L'accès accordé doit être en fonction du principe de droit d'accès minimal et accordé à une ressource unique. Les tentatives d'accès aux autres ressources nécessitent une nouvelle autorisation, avec des règles de vérification explicite différentes. Les administrateurs des organisations doivent déterminer comment appliquer les politiques d'accès aux ressources individuelles et les authentifications multicouches pour chaque demande d'accès.

4. **L'accès est fourni en fonction d'une politique dynamique basée sur le risque**

   L'accès à une ressource n'est pas un concept statique. Un utilisateur autorisé peut tout de même se voir refuser l'accès à une ressource particulière s'il existe une raison de croire que la demande d'accès est suspecte et qu'elle ne respecte pas les politiques établies.

   L'accès aux ressources est déterminé par des politiques dynamiques. Les personnes autorisées à accéder à une ressource doivent tout de même s'authentifier et prouver qu'elles répondent aux politiques de l'entreprise pour ouvrir une session. Pour ce faire, une combinaison des éléments suivants peut être exigée :

   - état et identité du client (y compris l'application, le service, le nom d'utilisateur et le mot de passe)
   - statut d'actif (adresse IP, réseau accédé, version logicielle, état des correctifs appliqués, géolocalisation, mises à jour installées)
   - autres critères nécessaires aux analyses (géolocalisation, motifs des demandes précédentes)

5. **Tous les actifs, qu'ils soient internes ou externes, sont surveillés en continu, en prenant soin de mesurer leur intégrité et leur posture de sécurité**

   Il n'y a aucun actif qui bénéficie d'une confiance inhérente, et chaque réseau et appareil est toujours considéré comme étant vulnérable à une attaque. Les organisations doivent se doter d'une surveillance robuste et d'un système de signalement afin d'être en mesure d'évaluer en continu la posture de sécurité des actifs après la réception d'une demande particulière d'accès. Les organisations doivent mettre en œuvre des techniques d'atténuation des risques et appliquer des correctifs lorsque nécessaire.

6. **Toutes les authentifications et les autorisations des ressources sont dynamiques et appliquées de façon stricte, avant d'accorder un accès**

   Votre organisation doit vérifier explicitement chaque tentative d'accès à une ressource. Balayer et vérifier les menaces, et réévaluer régulièrement la confiance, font partie d'un processus de surveillance continue. Une organisation doit disposer de mécanismes de justificatif d'identité, de gestion d'accès et de gestion des actifs.

   La mise en œuvre de l'AMF, combinée à une surveillance continue, est nécessaire pour s'assurer d'une réauthentification et d'une réautorisation, comme défini par les politiques de sécurité.

7. **Autant de données que possible sont recueillies concernant l'état actuel des actifs, de l'infrastructure réseau et des communications afin d'améliorer la posture de sécurité de l'organisation**

   Les organisations doivent collecter autant de données que possible à propos de l'état actuel du réseau et des communications pour améliorer la posture de sécurité de leur architecture en général. Les connaissances fournies par ces données permettront à votre organisation d'apprendre en continu et de toujours améliorer ses paramètres et ses politiques de sécurité dans le but de réduire les risques et d'appliquer une protection proactive.

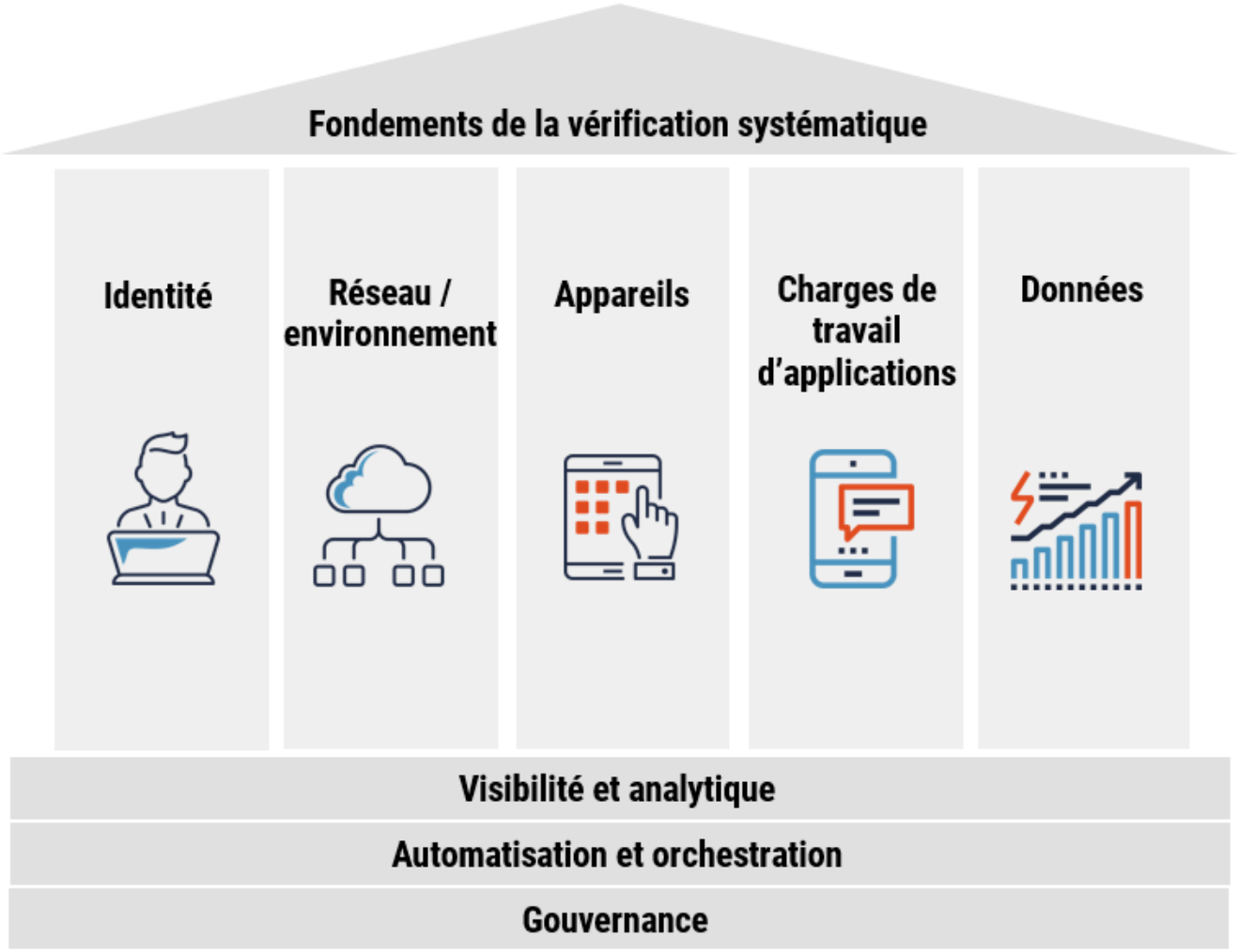
6.2 CISA : Modèle de maturité de l'approche à vérification systématique

L'ébauche du modèle de sécurité de la CISA a été publiée en juin 2021 en réponse au décret présidentiel sur la cybersécurité 14028. Le modèle est composé de cinq piliers : identité, appareil, réseau, charge de travail d'application et données. Chaque pilier comprend également des détails généraux concernant la visibilité et les analyses, l'automatisation, l'orchestration et la gouvernance. Ce modèle de sécurité est un des nombreux parcours soutenant une transition vers un MVS. Au sein de chaque pilier, le modèle de maturité offre des exemples d'AVS traditionnelles, évoluées et optimales. L'objectif des agences fédérales devrait être tourné vers une transition incrémentielle en vue d'une AVS, et éventuellement favoriser l'optimisation de la cybersécurité.

Il est à noter que la CISA continue d'évaluer et de modifier son modèle de maturité afin de mieux l'aligner à son programme de diagnostics et d'atténuation continus (CDM pour Continuous Diagnostics and Mitigation en anglais).

Voici ci-dessous la représentation des fondements d'une approche à vérification systématique de la CISA ainsi qu'une description de haut niveau des cinq piliers.

Figure 1: Représentation des fondements d'une approche à vérification systématique de la CISA



1. **Identité** : Les organisations doivent mettre en œuvre des technologies qui vérifient en continu l'identité afin d'accorder ou de refuser un accès. La vérification d'identité et l'authentification doivent être basées sur la demande d'accès et, si l'accès est accordé, celui-ci doit être d'une durée limitée et s'appliquer uniquement à la ressource demandée.

2. **Appareil** : Le terme « appareil » comprend tout actif matériel pouvant être connecté à un réseau, y compris les dispositifs de l'Internet des objets (IdO), les téléphones mobiles, les ordinateurs portables et les serveurs. Il est nécessaire de créer un inventaire de tous les appareils connectés, de consigner les accès et de surveiller la conformité et la validation de la posture de sécurité des appareils.

    a. Il est essentiel de non seulement s'assurer de l'intégrité de ces appareils, mais également des utilisateurs associés.

3. **Environnement réseau :** Un environnement réseau est un système de communication ouvert qui relie les utilisateurs entre eux et qui permet le partage de données. Les canaux de communication, à la fois ceux internes et externes, doivent être contrôlés, segmentés et protégés en fonction de leurs exigences uniques. Les organisations doivent éviter les modèles de défense de périmètre traditionnels, comme les coupe-feu. Elles doivent plutôt adopter des mesures comme le contrôle de l'accès, l'authentification continue, le chiffrement et l'évaluation des risques.

4. **Charge de travail d'application :** La charge de travail d'application est composée des systèmes d'agence, des programmes informatiques et des services qui sont exécutés sur place et dans l'environnement infonuagique. Toutes les applications doivent subir des essais empiriques rigoureux durant les étapes de développement et de déploiement pour assurer une protection contre les menaces. Le principe de droit d'accès minimal doit être appliqué durant tout le cycle de vie des applications.

5. **Données :** Les données provenant des appareils, des réseaux, des applications et du nuage doivent être protégées contre les menaces. Un inventaire de ces données doit être vérifié en continu en fonction d'un système d'étiquetage, de catégories et de suivi robuste.

Pour faciliter la transition vers un MVS en fonction des cinq piliers, la CISA propose un gradient de maturité en trois étapes, où chacune représente un niveau d'engagement de plus en plus important. La CISA a fourni les descriptions suivantes pour chaque étape afin d'identifier le niveau de maturité de chacun des piliers technologiques du MVS et d'assurer l'uniformité au sein du modèle de maturité :

- Traditionnel : Configurations et affectations manuelles des privilèges, politiques de sécurité statiques, solutions au niveau du pilier avec des dépendances grossières aux systèmes externes, principe de droit d'accès minimal établi lors du provisionnement, piliers exclusifs et rigides pour l'application de la politique, intervention en cas d'incident et déploiement manuel des mesures d'atténuation.
- Avancé : Coordination entre certains piliers, visibilité centralisée, contrôle de sécurité centralisé, application de politique basée sur les entrées et sorties entre les piliers, certaines interventions en cas d'incident associées à des mesures d'atténuation prédéfinies, dépendances des systèmes externes plus détaillées, modification de certains privilèges de droit d'accès minimal en fonction des évaluations de la posture.
- Optimal : Approche entièrement automatisée des privilèges associés aux actifs et aux ressources, politiques dynamiques basées sur des déclencheurs automatisés, actifs présentant des dépendances autoénumérables pour l'accès en fonction des privilèges de droit d'accès minimal (avec seuils), alignement en fonction des normes ouvertes pour l'interopérabilité entre les piliers, visibilité centralisée avec fonctionnalité d'historique pour un rétablissement d'état ponctuel périodique.

Le tableau 1 illustre une vue d'ensemble du modèle de maturité au sein de chaque étape de maturité des cinq piliers.

Tableau 1: Modèle de maturité de haut niveau de l'approche à vérification systématique de la CISA

Niveau de maturité	Identité	Dispositif	Réseau/ Environnement	Charge de travail d'application	Données
Traditionnel	• Mot de passe et authentification multifacteur (AMF) • Évaluation des risques limitée	• Visibilité limitée de la conformité • Inventaire simple	• Macro-segmentation • Chiffrement du trafic interne et externe minimal	• Accès basé sur l'autorisation locale • Intégration minimale au flux de travaux • Accessibilité au nuage limitée	• Inventaire limité • Contrôle statique • Non chiffré
Avancé	• AMF • Fédération d'identité limitée avec les systèmes infonuagique et sur site	• Application de la conformité • Accès aux données selon la posture des appareils lors du premier accès	• Micropérimètres d'entrée et de sortie définis • Analyse de base	• Accès basé sur une authentification centralisée • Intégration de base au flux de travaux d'application	• Contrôles basés sur les droits d'accès minimaux • Données stockées dans le nuage ou dans des environnements distants chiffrées au repos
Optimal	• Validation continue • Analyses d'apprentissage automatique en temps réel	• Surveillance et validation continues de la sécurité des appareils • Accès aux données dépendant des analyses de risque en temps réel	• Micropérimètres d'entrée et de sortie entièrement distribués • Protection des menaces basée sur l'apprentissage automatique • Trafic entièrement chiffré	• Accès autorisé en continu • Intégration étendue au flux de travaux d'application	• Soutien dynamique • Données entièrement chiffrées

6.3 NCSC : Principes de conception d'AVS

Les lignes directrices qui suivent ont été mises au point pour aider les professionnels et les responsables de la cybersécurité à concevoir et à évaluer une AVS qui répond à leurs exigences d'affaires. Le NCSC décrit une AVS comme étant « une approche où la confiance inhérente du réseau a été retirée; le réseau est ainsi considéré hostile et chaque demande est vérifiée en fonction des politiques d'accès ».

Voici les huit principes présentés dans le document d'aide de l'approche à vérification systématique de l'agence du Royaume-Uni.

1. **Connaître l'architecture, y compris les utilisateurs, les appareils, les services et les données**

   La première étape de développement d'une AVS est d'identifier tous les actifs et les composants de votre architecture, y compris les utilisateurs, les appareils, les services ainsi que les données accédées. Cela vous permettra de

déterminer où se trouvent vos ressources clés, où sont stockées vos données ainsi que leur niveau de sensibilité. Connaître cette information vous aidera à développer des politiques d'accès efficaces et appropriées qui protégeront vos ressources précieuses.

2. **Connaître les identités des utilisateurs, des services et des appareils**

   Déterminez l'identité de tous les utilisateurs, services et appareils de votre architecture. Cela est important pour décider de qui aura accès à quoi pour les droits d'accès aux données ou aux ressources.

3. **Évaluer le comportement des utilisateurs et des appareils ainsi que l'état des services**

   Il est très important de surveiller en continu le comportement des services et des appareils afin de repérer les anomalies. Ces dernières sont un indicateur important de leur état de sécurité. Utiliser les outils de sécurité appropriés pour mesurer les comportements des utilisateurs et des appareils, ainsi que l'état du service, est la clé pour établir une AVS. Les outils aideront à évaluer le niveau de confiance et la fiabilité.

4. **Utiliser des politiques pour autoriser les demandes**

   Chaque demande de données ou de service doit être autorisée en fonction d'une politique. La puissance d'une AVS découle des politiques d'accès que vous définissez.

5. **Exploiter les mécanismes d'authentification et d'autorisation en tout temps**

   Les décisions d'authentification et d'autorisation doivent considérer plusieurs éléments, comme l'emplacement de l'appareil et son état ainsi que l'identificateur d'utilisateur et son état. Cela permettra d'évaluer le risque associé à la demande d'accès. Vous devez toujours supposer que le réseau est hostile et vous assurer que toutes les connexions qui accèdent à vos données ou à vos services sont authentifiées et autorisées.

6. **Centrer la surveillance sur les utilisateurs, les appareils et les services**

   Dans une AVS, la surveillance mise sur le comportement des utilisateurs, des appareils et des services. Cela vous aidera ainsi à établir leur état en matière de cybersécurité. Vous devez connaître les actions réalisées par appareils, les utilisateurs et les services, ainsi que les données concernées. Votre surveillance doit faire référence aux politiques que vous avez établies et vérifier qu'elles sont appliquées comme attendu.

7. **Ne faire confiance à aucun réseau, y compris le vôtre**

   Ne faites confiance à aucun réseau entre l'appareil et le service accédé, y compris le réseau local. Les communications d'un réseau pour l'accès à des données ou à des services doivent utiliser un protocole de transport sécurisé pour s'assurer que le trafic est protégé en transit. Il sera ainsi moins exposé aux menaces.

8. **Choisir des services conçus pour un MVS**

   Il se peut que les services ne prennent pas en charge l'approche à vérification systématique et que vous ayez besoin de ressources supplémentaires et de plus de temps à consacrer au soutien. Dans ces scénarios, il peut être prudent de considérer des produits et des services de rechange qui ont été conçus spécifiquement pour une approche à vérification systématique.

7 Résumé

Dans un paysage technologique en pleine évolution comptant des cybermenaces de plus en plus sophistiquées, il est plus important que jamais de migrer vers une AVS. Il faut savoir que le concept de vérification systématique ne s'applique pas à un produit, à une technologie ou à une couche d'architecture unique. Il représente plutôt une architecture de sécurité et une philosophie de conception dont le principe fondamental est qu'aucun sujet (application, utilisateur, appareil) n'est un système d'information de confiance par défaut. La confiance est réévaluée chaque fois qu'un sujet demande l'accès à une ressource. Le niveau d'accès accordé est rajusté de manière dynamique en fonction du degré de confiance établi pour l'élément.

La migration vers un MVS est un processus complexe qui peut nécessiter d'apporter des changements à tous les niveaux organisationnels. Cela nécessite de plus un engagement conjoint de la part de tous pour les efforts déployés. Malgré sa complexité, une telle migration permettra aux organisations d'améliorer de manière significative leur posture de sécurité.

Le présent document présente un aperçu des concepts de l'approche à vérification systématique ainsi que les comportements associés. Il permettra aux organisations de mieux comprendre le MVS dans son ensemble ainsi que les avantages et les défis connexes. Nous avons répertorié quelques pratiques exemplaires et principes à respecter pour la mise en œuvre d'un MVS. Nous présentons trois cadres et systèmes de lignes directrices MVS couramment cités afin d'aider les organisations à choisir ce qui convient le mieux à leurs exigences d'affaires, à leur infrastructure réseau et au contexte de menace qui s'applique.

8 Contenu complémentaire

8.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Définition
ABAC	Contrôle de l'accès basé sur les privilèges (Attribute-Based Access Control en anglais)
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
FSI	Fournisseur de services infonuagiques
PAP	Prenez vos appareils personnels
DoD	Department of Defense
DoDAF	Cadre architectural du Department of Defense (Department of Defense Architecture Framework en anglais)
EO	Décret présidentiel (Executive Order en anglais)
GC	Gouvernement du Canada
CI	Circuit intégré
IdO	Internet des objets
IP	Protocole IP (Internet Protocol en anglais)
TI	Technologies de l'information
AMF	Authentification multifacteur
NCSC	National Cyber Security Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PAM	Gestion des accès privilégiés (Privileged Access Management en anglais)
PAW	Poste de travail avec accès privilégié (Privilege Access Workstation en anglais)
PBAC	Contrôle de l'accès basé sur la sécurité (Policy-Based Access Controls en anglais)
PC	Ordinateur personnel (Personal Computer en anglais)
PoLP	Principe de droit d'accès minimal (Principle of Least Privilege en anglais)
RBAC	Contrôle d'accès basé sur les rôles (Role-Based Access Control en anglais)
SAW	Poste de travail administratif sécurisé (Secure Administrative Workstation en anglais)
SDP	Périmètre défini par logiciel (Software-Defined Perimeter en anglais)
GIES	Gestion des informations et des événements de sécurité
SCT	Secrétariat du Conseil du Trésor
TPM	Module de plateforme de confiance (Trusted Platform Module en anglais)
R.-U.	Royaume-Uni
É.-U.	États-Unis
VLAN	Réseau local virtuel (Virtual Local Area Network en anglais)
RPV	Réseaux privés virtuels
MVS	Modèle à vérification systématique
AVS	Architecture à vérification systématique

8.2 Glossaire

Terme	Définition
Contrôle d'accès	Attestation confirmant que seul un accès autorisé est donné aux biens (tant physiques qu'électroniques). Pour ce qui concerne les actifs physiques, le contrôle de l'accès peut s'appliquer aux installations ou aux zones d'accès limité (p. ex. filtrage des visiteurs et du matériel aux points d'entrée, escorte accompagnant les visiteurs). Pour ce qui concerne les actifs de TI, le contrôle de l'accès peut s'appliquer aux réseaux, aux systèmes ou à l'information (p. ex. restreindre le nombre des utilisateurs de certains systèmes ou limiter les autorisations d'accès attribuées à certains comptes).
Privilège d'administrateur	Autorisations qui permettent à un utilisateur d'exécuter certaines fonctions sur un système ou un réseau, comme l'installation d'un logiciel et la modification de paramètres de configuration.
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Autorisation	Droits d'accès accordés à un utilisateur, à un programme ou à un processus.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril sa confidentialité, son intégrité ou sa disponibilité.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Infonuagique	Recours à des serveurs distants hébergés dans l'Internet. L'infonuagique permet à des utilisateurs d'accéder à un ensemble de ressources informatiques (comme des réseaux, des serveurs, des applications, des services) sur demande et de n'importe où. Les utilisateurs parviennent à ces ressources par l'intermédiaire d'un réseau informatique plutôt que d'avoir à les stocker toutes sur leur propre ordinateur.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à infiltrer un système informatique, un réseau ou un dispositif.
Cybermenaces	Situation où un auteur de menace, utilisant Internet, profite d'une vulnérabilité connue dans un produit dans le but d'exploiter un réseau et les informations sur ce réseau.
Détection	Surveillance et analyse des événements d'un système en vue de relever les tentatives d'accès non autorisées aux ressources du système.
Chiffrement	Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.
Coupe-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre. Les ressources du système local sont ainsi protégées contre un accès de l'extérieur.
Intégrité	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

Terme	Définition
	s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Propriété intellectuelle	Droits légaux qui découlent de l'activité intellectuelle dans les domaines industriel, scientifique, littéraire et artistique. Des exemples incluent les droits d'auteur, les marques de commerce et les brevets.
Internet des objets	Réseau formé par les dispositifs Web utilisés couramment, qui peuvent se connecter les uns aux autres et qui peuvent se transmettre de l'information.
Actif TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
Droit d'accès minimal	Principe selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation accidentelle, incorrecte ou non autorisée d'un système d'information.
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
Authentification multifacteur	L'authentification est validée par la conjugaison de deux ou plusieurs facteurs parmi les suivants : une information connue (p. ex. un mot de passe); une possession (p. ex. un jeton physique); un attribut personnel (p. ex. la biométrie).
Zone de sécurité de réseau	Environnement de réseau clairement délimité relevant d'une autorité de zone de sécurité de réseau et caractérisé par un niveau standard de vulnérabilité aux menaces. On distingue les types de zones d'après les exigences de sécurité s'appliquant aux interfaces, au contrôle du trafic, à la protection des données, au contrôle de la configuration de l'hôte et au contrôle de la configuration du réseau.
Périmètre	Frontière entre deux zones de sécurité de réseau par laquelle le trafic est acheminé.
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 actifs TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des politiques, des pratiques et des procédures de sécurité.

8.3 Références

Numéro	Référence
1	National Institute for Standards and Technology. Special Publication 800-207: Zero Trust Architecture, août 2020.
2	Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model, juin 2021
3	National Cyber Security Center : Zero trust architecture design principles, juillet 2021
4	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.
5	Centre canadien pour la cybersécurité. Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030), juin 2020

Numéro	Référence
6	Centre canadien pour la cybersécurité. Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3), avril 2018
7	Secrétariat du Conseil du Trésor. Ligne directrice sur la définition des exigences en matière d'authentification, novembre 2012
8	Décret présidentiel Executive Order (EO) 14028 to Improve the Nation's Cybersecurity, mai 2021