Modèle à vérification systématique (ou architecture zéro confiance)

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Novembre 2022 | ITSAP.10.008

Le modèle de sécurité typique qu'appliquaient auparavant les organisations pour protéger les systèmes d'information reposait sur la défense du périmètre et faisait implicitement confiance à toutes les personnes se trouvant à l'intérieur du réseau organisationnel, à qui l'on accordait alors un accès aux ressources. Comme de plus en plus de gouvernements et d'entreprises poursuivent leur transformation numérique en adoptant des technologies basées sur l'infonuagique et des modes travail à distance ou hybrides, les mesures de défense conventionnelles axées sur le périmètre ne suffisent plus à protéger les réseaux et les données internes. Le présent document fournit de l'information sur le modèle à vérification systématique (ou architecture zéro confiance [ZTA]) et la manière dont il permet de relever les défis d'aujourd'hui liés à la sécurisation du personnel travaillant à distance, aux environnements infonuagiques hybrides et aux menaces pour la cybersécurité.

Qu'est-ce que le modèle à vérification systématique?

Le terme "modèle à vérification systématique" (MVS) ne correspond pas à un produit, à une technologie ou à une couche d'architecture en particulier. Il représente plutôt un cadre de sécurité visant à protéger l'infrastructure et les données. Selon le principe central du MVS, aucun élément (application, utilisateur ou appareil) d'un système d'information n'est digne de confiance par défaut. Il faut réévaluer et vérifier la confiance chaque fois qu'un élément demande l'accès à une nouvelle ressource. Le niveau d'accès accordé est rajusté de manière dynamique en fonction du degré de confiance établi pour l'élément en question. Le MVS consiste à adopter une nouvelle façon de voir la sécurité en anticipant toujours une atteinte à la sécurité et en privilégiant la protection des ressources (comme les services et les données). Dans le contexte de l'évolution constante de la technologie et de l'apparition de cybermenaces toujours plus sophistiquées et persistantes, le modèle à vérification systématique peut aider les organisations à renforcer considérablement leur cyberdéfense.

Le gouvernement du Canada (GC) élabore actuellement un cadre de sécurité axé sur le MVS qui repose sur le modèle de la Cybersecurity and Infrastructure Security Agency (CISA) et la publication spéciale du National Institute of Standards and Technology (NIST). Ce cadre présente notamment les concepts et les éléments du MVS que peuvent mettre en œuvre les ministères et organismes pour améliorer la posture de sécurité globale du GC.

> "Ne jamais se fier, toujours vérifier"

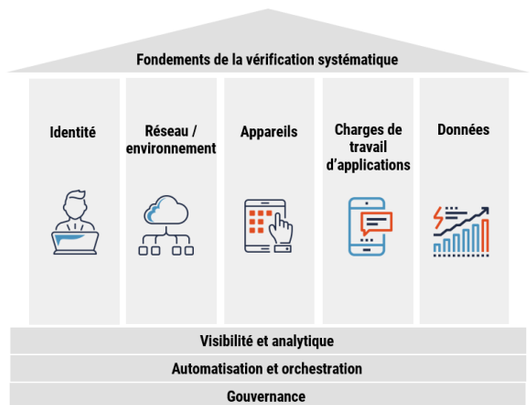
Modèle de maturité à vérification systématique de la CISA

La CISA des États-Unis propose un MVS (en anglais seulement) constitué de cinq piliers et de trois capacités. Ce modèle est conçu pour fournir aux organisations une feuille de route et des ressources qui les aideront à établir un environnement à vérification systématique optimal au fil du temps.

Identité. Mettre en œuvre des mécanismes d'authentification multifacteur (AMF) qui résistent à l'hameçonnage et valider en continu les utilisateurs et les entités tout au long de leurs interactions avec les services ou les données. Utiliser des identités gérées par l'entreprise dans les environnements locaux et infonuagiques. Appliquer le principe de droit d'accès minimal.

Réseau/environnement. Mettre en œuvre la microsegmentation pour isoler les données critiques des autres données. Contrôler l'accès privilégié au réseau, gérer les flux de données (internes et externes) et chiffrer l'ensemble du trafic et des connexions.

Appareils. Établir des mesures de protection de base pour les appareils. Surveiller et valider en continu la sécurité des appareils. Utiliser les données d'analyse de l'apprentissage automatique afin de prendre des décisions sur le contrôle de l'accès pour les services et les données. Effectuer régulièrement l'inventaire des appareils.



Charges de travail d'applications. Autoriser en continu l'accès aux applications. Intégrer fortement les mesures de protection contre les menaces aux flux de travaux des applications. Intégrer les tests de sécurité d'applications tout au long du processus de développement et de déploiement.

Données. Protéger les données contenues dans les appareils, les applications et les réseaux. Dresser l'inventaire des données, puis les catégoriser et les étiqueter, et déployer des mécanismes permettant de détecter l'exfiltration de données. Chiffrer toutes les données au repos ou en transit (dans les environnements infonuagiques ou distants).

Visibilité et analytique. Employer des outils comme des plateformes d'analytique de sécurité évoluée et des données d'analyse des comportements d'utilisateurs pour observer et analyser en temps réel les comportements des utilisateurs et l'état de santé des services et des appareils. Journaliser et analyser tous les événements d'accès pour détecter les comportements suspects.

Automatisation et orchestration. Automatiser les processus opérationnels de sécurité et de réseau en gérant les fonctions entre tous les systèmes de sécurité et toutes les applications. Mettre en œuvre des contrôles d'accès juste-à-temps et juste-assez. Appliquer automatiquement des contrôles d'accès stricts pour les données de grande valeur.

Gouvernance. Automatiser l'application des mesures de protection des données exigées par les politiques. Utiliser la découverte automatisée des réseaux, des appareils et des services au moyen de l'autorisation manuelle ou dynamique et de l'élimination automatisée des entités non autorisées.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

© Gouvernement du Canada | Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production ou publication, en tout ou en partie, est stritement interdite sans l'autorisation expresse du CST. No de cat.D97-1/10-008-2022F-PDF ISBN 978-0-660-45919-6

Modèle à vérification systématique (ou architecture zéro confiance)

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Novembre 2022 | ITSAP.10.008

Quels sont les avantages du MVS ?

Bien qu'aucune stratégie de sécurité ne soit parfaite et qu'il existera toujours des cybermenaces, le MVS constitue une approche efficace pour améliorer la posture de cybersécurité d'une organisation dans le contexte de la transformation numérique d'aujourd'hui. Voici quelques avantages du MVS:

- **Sécurité accrue du réseau**. Chaque interaction numérique (comme la connexion d'un utilisateur à une application) est vérifiée et autorisée en continu pour veiller à ce que les conditions établies dans les politiques de sécurité d'une organisation soient remplies. Lorsque cette façon de faire est jumelée à la segmentation réseau et à des mécanismes robustes d'authentification d'utilisateurs et d'appareils, elle permet d'améliorer la sécurité globale du réseau.
- **Atténuation des répercussions de violations de données**. Grâce à l'adoption de zones de confiance plus petites, les auteurs de cybermenace doivent se soumettre à l'authentification et à l'autorisation pour franchir une nouvelle frontière de sécurité chaque fois qu'ils accèdent à une ressource différente. Cela limite leurs déplacements latéraux dans un réseau et réduit l'ampleur d'une éventuelle violation de données.
- **Meilleure protection des données**. Le MVS repose sur des technologies comme le chiffrement robuste, des réseaux privés virtuels (RPV) et des capacités de prévention de la perte de données afin de protéger les données au repos et en transit.
- **Conformité en continu.** L'amélioration de la visibilité des éléments "qui, quoi, où" permet aux opérateurs réseau de journaliser les comportements et les activités avec une plus grande précision dans le but de vérifier la conformité aux stratégies.
- **Amélioration de la visibilité, de la détection et de l'intervention.** La journalisation et la surveillance automatiques des cyberévénements provenant des appareils d'utilisateurs et de services permettent d'obtenir une vue d'ensemble de l'environnement en temps réel. L'analytique améliore la visibilité dont disposent les opérateurs réseau, ce qui les aide à développer des mesures de sécurité proactives avant que des incidents se produisent ou à réagir rapidement en cas de menace.
- **Solution sécurisée à l'appui de la modernisation de l'effectif.** Le MVS soutient de nouvelles façons de travailler, car il permet de connecter en toute sécurité des utilisateurs, des appareils, des applications et des services sur un réseau (qu'il s'agisse d'un environnement local ou en nuage public ou hybride) au moyen de stratégies de validation basées sur l'identité.

Pour en savoir plus sur l'architecture, les lignes directrices et les cadres liés au MVS, consultez les ressources suivantes:

- SP 800-207: Zero Trust Architecture du NIST (en anglais seulement)
- Zero Trust Maturity Model de la CISA (en anglais seulement)
- SP 1800-35: Implementing a Zero Trust Architecture (Preliminary Draft) du NIST (en anglais seulement)
- Zero trust architecture design principles du National Cyber Security Centre du Royaume-Uni (en anglais seulement)
- Essential Eight Maturity Model de l'Australian Cyber Security Centre (en anglais seulement)

Quels sont les défis liés au MVS ?

Les organisations qui souhaitent améliorer leur posture de sécurité au moyen du MVS devront tenir compte de certains défis potentiels, notamment :

- **Il faut investir du temps et des efforts** pour authentifier chaque utilisateur et appareil au moyen de l'authentification à deux facteurs. Cela nécessite un travail technique et administratif considérable à l'échelle de plusieurs organisations pour définir et mettre en œuvre les attributs détaillés de chaque utilisateur et ressource à l'appui des décisions sur la confiance et l'accès.
- **Il faut maintenir le cap et l'engagement au niveau organisationnel** sur plusieurs années, ce qui peut rendre la mise en place du MVS difficile. Le MVS touche plusieurs niveaux d'infrastructure et d'activités, et il faut assurer une coordination étroite pour réussir.
- **Les organisations sont plus susceptibles d'être contraintes à utiliser à long terme les systèmes exclusifs des fournisseurs de services infonuagiques.** Les organisations qui font appel à des solutions dans de multiples nuages risquent d'être confrontées à de tels défis, car le MVS est un cadre plutôt qu'une norme de l'industrie. Il est essentiel d'établir des partenariats avec des fournisseurs de services infonuagiques commerciaux afin de bien comprendre les objectifs opérationnels et de sécurité de l'organisation et de choisir la solution appropriée.

Comment passer à un MVS ?

Pour améliorer la posture de cybersécurité de votre organisation, vous pouvez suivre les étapes suivantes afin de lancer votre transition vers le MVS:

Appliquer des mécanismes d'AMF robustes. Viser le niveau d'assurance 3. Pour en savoir plus, consultez notre publication intitulée Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3).

Employer des stratégies adaptatives axées sur le risque qui reposent sur l'accès juste-à-temps et juste-assez pour mettre en œuvre le principe de droit d'accès minimal.

Accorder l'accès en fonction de l'information sur l'utilisateur et l'appareil et non uniquement selon l'emplacement logique. Utiliser de multiples points de données (par exemple, l'identité, l'emplacement, la santé de l'appareil, la ressource, la classification des données et les anomalies) afin de prendre des décisions sur la sécurité.

Utiliser des dispositifs dédiés, des postes de travail à accès privilégié (PAW pour *Privileged Access Workstation*) et des postes de travail d'administrateur sécurisés (SAW pour *Secured Admin Workstations*) pour séparer les tâches et les comptes sensibles des activités non administratives comme le courriel et la navigation Web.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

© Gouvernement du Canada | Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production ou publication, en tout ou en partie, est stritement interdite sans l'autorisation expresse du CST. No de cat.D97-1/10-008-2022F-PDF ISBN 978-0-660-45919-6