CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-08(24)

Défaillance et reprise sécurisées

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-08(24) — Défaillance et reprise sécurisées (PbMM)

Énoncés :

Mettre en place le principe de conception sécurisée de la défaillance et de la reprise sécurisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de défaillance et de reprise sécurisées repose sur le fait que ni la défaillance d'une fonction ou d'un mécanisme d'un système ni la reprise effectuée advenant une défaillance ne saurait donner lieu à la violation d'une stratégie de sécurité. Le principe de défaillance et de reprise sécurisées est similaire au principe de protection continue qui vise à s'assurer qu'un système est en mesure de détecter (dans les limites fixées) les défaillances actuelles et imminentes à toutes les étapes de son exécution (c'est-à-dire l'initialisation, l'exécution normale, l'arrêt et la maintenance) et à prendre les mesures appropriées pour veiller à ne pas enfreindre les stratégies de sécurité. Dans les cas précisés, le système est de plus capable de rétablir ses activités après une défaillance actuelle ou imminente afin d'assurer une reprise des activités sécurisées normales, dégradées ou autres tout en veillant à ce qu'un état sécurisé soit maintenu de manière à ne pas enfreindre les stratégies de sécurité. Une défaillance est une condition dans le cadre de laquelle le comportement d'un composant déroge du comportement indiqué ou attendu pour le résultat explicitement documenté. Advenant la détection d'une fonction de sécurité défaillante, le système peut se reconfigurer de manière à contourner le composant défectueux tout en maintenant la sécurité et à fournir la totalité ou une partie de la fonctionnalité au système d'origine, ou il peut s'éteindre entièrement pour éviter d'enfreindre davantage les stratégies de sécurité. Pour ce faire, les fonctions de reconfiguration du système sont conçues pour assurer une application continue de la stratégie de sécurité au cours des diverses phases de reconfiguration. Une autre technique à utiliser pour assurer la reprise advenant des défaillances consiste à procéder à une restauration à un état sécurisé (lequel peut correspondre à l'état initial), puis à éteindre ou à remplacer le service ou le composant défaillant de manière à pouvoir reprendre les activités sécurisées. La défaillance d'un composant peut être détectée ou non par les composants qui l'utilisent. Le principe de défaillance sécurisée veut que les composants plantent dans un état qui refuse l'accès plutôt que de l'autoriser. Par exemple, une opération nominalement atomique qui est interrompue avant sa complétion n'enfreint pas la stratégie de sécurité et est conçue de manière à gérer les événements d'interruption en faisant appel à un niveau d'atomicité plus élevé et à des mécanismes de restauration (par exemple, des transactions). Si un service est utilisé, ses propriétés d'atomicité sont bien documentées et caractérisées de manière à ce que le composant qui a recours à ce service puisse détecter et gérer les événements d'interruption de façon appropriée. Par exemple, un système est conçu pour répondre en douceur à la déconnexion et prendre en charge la resynchronisation et l'uniformité des données après la déconnexion. Les stratégies de protection contre les défaillances qui font appel à la réplication des mécanismes d'application des stratégies (ce qu'on appelle parfois la défense en profondeur) peuvent permettre au système de continuer à un état sécurisé même si un mécanisme n'a pas réussi à le protéger. Si les mécanismes sont similaires, par contre, la protection additionnelle peut être illusoire, car l'adversaire n'a qu'à mener une série d'attaques. Dans un système en réseau, percer la sécurité d'un système ou d'un service peut permettre à un attaquant de faire la même chose pour tous les autres systèmes et services reproduits qui sont similaires. En utilisant plusieurs mécanismes de protection aux fonctions considérablement différentes, on peut réduire la probabilité qu'une attaque soit répliquée ou répétée. Des analyses sont effectuées pour évaluer les coûts et les avantages de telles techniques de redondance par rapport à l'utilisation accrue des ressources et aux effets négatifs sur les performances globales du système. Des analyses supplémentaires sont effectuées à mesure que la complexité de ces mécanismes augmente, comme ça pourrait être le cas pour les comportements dynamiques. Une complexité accrue réduit généralement la robustesse. Lorsqu'une ressource ne peut pas faire l'objet d'une protection continue, il est capital de détecter et de réparer toute brèche de sécurité avant que la ressource soit utilisée de nouveau dans un contexte sécurisé.