CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

RA-05

Surveillance et analyse des vulnérabilités

Juill. 2026

Votre gouvernement

Québec

RA

Évaluation des risques

Risk Assessment

RA-05 — Surveillance et analyse des vulnérabilités (PaFF) (Obligatoire)

Énoncés :

a. Surveiller et analyser les vulnérabilités dans le système et les applications hébergées [Affectation : fréquence définie par l'organisation ou de manière aléatoire conformément au processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système sont identifiées et signalées
b. Utiliser des outils et des techniques de surveillance des vulnérabilités qui facilitent l'interopérabilité et automatisent les composantes du processus de gestion des vulnérabilités en appliquant des normes sur :
1. les relevés des plateformes, des lacunes logicielles et des configurations inappropriées
2. le formatage des listes de vérification et des procédures de test
3. la mesure de l'incidence des vulnérabilités
c. Analyser les rapports d'analyse des vulnérabilités et les résultats de la surveillance des vulnérabilités
d. Corriger les vulnérabilités légitimes [Affectation : temps de réponse défini par l'organisation] conformément à l'évaluation des risques de l'organisation
e. Communiquer l'information découlant du processus de surveillance des vulnérabilités et des évaluations des contrôles à [Affectation : personnel ou rôles définis par l'organisation] pour faciliter l'élimination de vulnérabilités semblables dans les autres systèmes
f. Employer des outils de surveillance des vulnérabilités qui sont dotés de la capacité de mettre à jour rapidement les vulnérabilités à analyser

Paramètres :

a. fréquence définie en fonction du service gouvernemental de balayages de vulnérabilités *b. Adhérer au service gouvernemental de balayages de vulnérabilités pour l'ensemble des actifs informationnels, qu'ils soient exposés ou non à Internet.
d. dans les délais prescrits par le processus de gestion des menaces, vulnérabilités et incidents (GMVI)
e. responsables définis dans le processus de gestion des menaces, vulnérabilités et incidents (GMVI)

Responsable : Partagée

Date limite de mise en oeuvre : 2021-06-30

Discussion :

La catégorisation de la sécurité de l'information et des systèmes aide à définir la fréquence et le niveau d'exhaustivité de la surveillance des vulnérabilités (y compris des analyses). Les organisations devraient déterminer la surveillance des vulnérabilités requise pour les composants des systèmes et s'assurer que les sources potentielles de vulnérabilités, comme les composants des infrastructures (par exemple, les commutateurs, les routeurs, les mécanismes de protection, les capteurs), les imprimantes, les numériseurs et les photocopieurs en réseau, ne sont pas ignorées. La capacité permettant d'actualiser aisément les outils de surveillance des vulnérabilités à mesure que de nouvelles vulnérabilités sont découvertes, annoncées, et que de nouvelles méthodes d'analyse sont établies, aide à s'assurer que les nouvelles vulnérabilités sont prises en compte par les outils de surveillance des vulnérabilités employés. Le processus de mise à jour de la surveillance des vulnérabilités permet d'identifier les éventuelles vulnérabilités auxquelles s'exposent les systèmes et d'intervenir dans les plus brefs délais. Les analyses et la surveillance des vulnérabilités visant les logiciels sur mesure pourraient nécessiter des mesures additionnelles, comme des analyses statiques, des analyses dynamiques, des analyses binaires ou encore des analyses recourant à une combinaison de ces trois approches. Les organisations peuvent utiliser ces analyses dans les examens de code source et dans divers outils, notamment dans les outils d'analyse statique, les analyseurs d'application Web et des analyseurs binaires. La surveillance des vulnérabilités comprend l'analyse des niveaux de correctifs; l'analyse des fonctions, des ports, des protocoles et des services qui ne doivent pas être accessibles aux utilisatrices et utilisateurs ou aux dispositifs; et l'analyse des mécanismes de contrôle de flux qui sont mal configurés ou défectueux. Cette surveillance peut également comprendre les outils de surveillance continue des vulnérabilités qui se servent de l'instrumentation pour analyser sans cesse les composants. Les outils axés sur l'instrumentation peuvent améliorer la précision et fonctionner dans l'ensemble de l'organisation sans avoir recours à l'analyse. Parmi les outils de surveillance des vulnérabilités qui facilitent l'interopérabilité, on retrouve ceux qui sont validés par le protocole SCAP (Security Content Automated Protocol). Ainsi, les organisations devraient considérer l'utilisation d'outils d'analyse qui expriment les vulnérabilités selon la convention d'appellation des vulnérabilités et expositions courantes (CVE pour Common Vulnerabilities and Exposures) et qui emploient l'analyse OVAL (Open Vulnerability Assessment Language) pour déceler la présence de vulnérabilités. Les sources d'information sur les vulnérabilités comprennent la liste des lacunes courantes (CWE pour Common Weakness Enumeration) et la base de données nationale sur les vulnérabilités (NVD pour National Vulnerability Database). Des évaluations des contrôles, comme les exercices effectués par l'équipe de testeuses et testeurs, donnent des sources additionnelles de vulnérabilités possibles à analyser. Les organisations devraient aussi envisager le recours à des outils d'analyse qui expriment l'incidence des vulnérabilités par l'entremise du système de notation des vulnérabilités courantes (CVSS pour Common Vulnerability Scoring System). La surveillance des vulnérabilités

comprend un canal et un processus permettant d'obtenir des rapports des vulnérabilités informatiques provenant du grand public. Les programmes de divulgation des vulnérabilités peuvent être aussi simples que la publication d'une adresse courriel surveillée. Il pourrait aussi s'agir d'un formulaire Web permettant de recevoir des rapports, dont des notifications qui autorisent une recherche ou une divulgation de vulnérabilités informatiques faite de bonne foi. Les organisations s'attendent en général à ce qu'une telle recherche se fasse avec ou sans leur autorisation et qu'elles soient en mesure de se servir des canaux de divulgation des vulnérabilités pour accroître la probabilité que les vulnérabilités relevées soient signalées directement à l'organisation concernée pour lui permettre de les corriger. Les organisations peuvent également avoir recours à des incitatifs financiers (aussi appelés primes de bogues) pour inciter davantage les chercheuses et chercheurs en sécurité à signaler les vulnérabilités relevées. Des programmes de prime de bogues peuvent être adaptés en fonction des besoins de l'organisation. Les primes peuvent être en vigueur indéfiniment ou pour une période déterminée, et elles peuvent être offertes au grand public ou à un groupe prédéterminé. Les organisations peuvent exécuter des programmes de prime de bogues privés ou ouverts au public simultanément et pourraient choisir d'offrir un accès avec justificatifs d'identité à des participantes et participants afin d'évaluer les vulnérabilités informatiques de points de vue privilégiés.