|  |  |  |
| --- | --- | --- |
| logo | Plan de test | 1088 |

Responsable :

Mis à jour :

Les tests de sécurité sont définis et mis en œuvre dans le cycle de vie du développement afin de valider le respect des exigences de sécurité de l’information lorsque des applications ou du code sont déployés dans l'environnement de production.

Les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions sont minutieusement testés et vérifiés au cours des processus de développement.

Les tests de sécurité font partie intégrante des tests de systèmes ou de composants.

Les tests de sécurité sont menés par rapport à un ensemble d'exigences, qui peuvent être fonctionnelles ou non fonctionnelles.

Les tests de sécurité vérifient :

* les fonctions de sécurité (authentification de l'utilisateur, restriction d'accès, utilisation de la cryptographie)
* le codage sécurisé
* les configurations sécurisées (systèmes d'exploitation, pare-feu et autres composants de sécurité)

L'étendue des tests est proportionnelle à l'importance, à la nature du système et à l'impact potentiel du changement introduit.

Exemple de plan de test :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Activités | Date | Entrées | Sorties | Conditions | Critères d’évaluation | Résultats | Action |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

L'organisation peut utiliser des outils automatisés (analyse de code ou scanners de vulnérabilité) et vérifie la correction des défauts liés à la sécurité.

Pour les développements internes, ces tests sont effectués par l'équipe de développement et ensuite des tests d'acceptation indépendants sont réalisés afin de s'assurer que le système fonctionne comme prévu et uniquement comme prévu.

Les éléments suivants sont pris en compte :

* effectuer des activités de révision du code en tant qu'élément pertinent pour tester les failles de sécurité, y compris les entrées et les conditions imprévues
* effectuer une analyse des vulnérabilités pour identifier les configurations non sécurisées et les vulnérabilités du système
* effectuer des tests d'intrusion pour identifier le code et la conception non sécurisés

Pour les composants de développement et d'achat externalisés, un processus d'acquisition est utilisé. Les contrats avec le fournisseur répondent aux exigences de sécurité identifiées. Les produits et services sont évalués par rapport à ces critères avant l'acquisition.

Les tests sont effectués dans un environnement de test qui correspond le plus possible à l'environnement de production cible pour s'assurer que le système n'introduit pas de vulnérabilités et que les tests sont fiables.

Plusieurs environnements de test peuvent être établis, qui peuvent être utilisés pour différents types de tests (tests fonctionnels et de performance). Ces différents environnements peuvent être virtuels, avec des configurations individuelles pour simuler une variété d'environnements d'exploitation.