

Services d'assurance de la sécurité applicative

État actuel de l'industrie

- « Plus de 70 % des vulnérabilités en matière de sécurité se trouvent à la couche applicative et non pas à la couche réseau. » (Gartner)
- « La bataille entre les pirates informatiques et les professionnels de la sécurité est passée de la couche réseau aux applications Web elles-mêmes. » (Network World)
- « Les pertes financières découlant d'applications Web vulnérables sont importantes; elles peuvent s'élever jusqu'à 60 G\$ par année. » (IDC/IBM Systems Sciences Institute)
- « Environ 64 % des développeurs ne sont pas certains d'être en mesure d'élaborer des applications sécurisées. » (Microsoft Developer Research)

Règles gouvernementales et de l'industrie en matière de sécurité

- Loi Sarbanes-Oxley (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gram-Leach-Bliley Act
- Payment Card Industry Data Security Standard (PCI-DSS)
- Federal Information Security Management Act (FISMA)
- COBIT et ISO 17799

SÉCURITÉ APPLICATIVE

Aujourd'hui, les organisations tirent de plus en plus profit d'Internet pour réaliser leurs opérations d'affaires quotidiennes qui sont essentielles et pour interagir avec leurs parties prenantes. Les opérations commerciales et les données sensibles ou privées franchissent rapidement et aisément les quatre murs de l'entreprise.

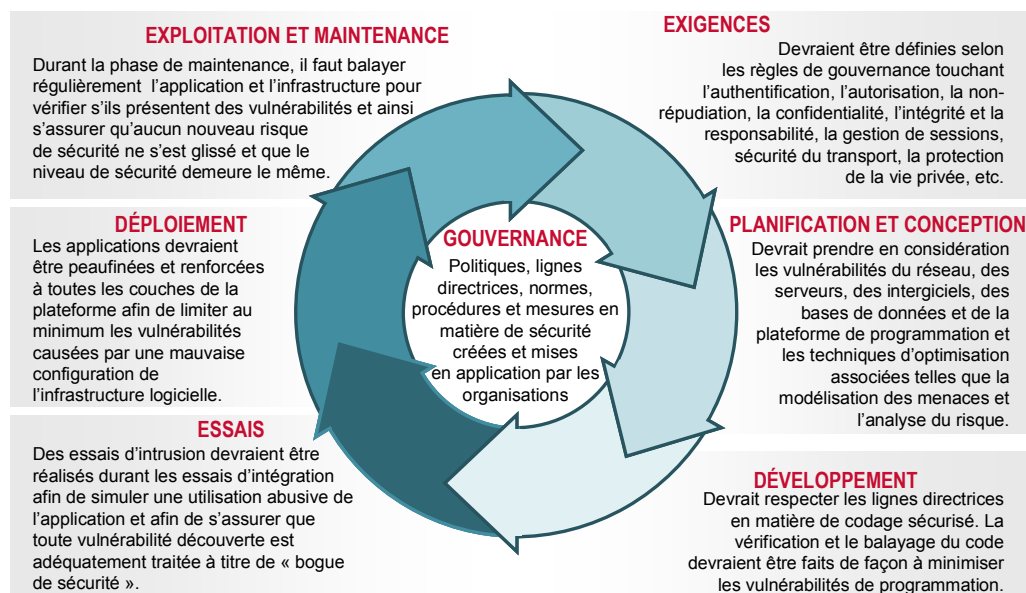
Les applications des organisations ne jouent plus uniquement le rôle d'outil; il s'agit d'atouts importants pour l'entreprise et elles constituent sa marque et sa capacité de générer un avantage concurrentiel. Protéger ces atouts nécessite une approche rigoureuse et axée sur la gestion des risques et l'assurance de la sécurité.

Les pirates informatiques se détournent des réseaux et des serveurs pour se concentrer sur les applications. Toutefois, la sécurité des applications n'est pas adéquatement prise en charge. Après les fonctionnalités et la performance vient la sécurité, qui est considérée comme le troisième pilier de la qualité d'une application.

Si la gravité de la menace informatique sur les applications d'entreprise ne suffit pas à changer les mentalités à l'égard de la sécurité des applications, alors les exigences réglementaires et les règles plus strictes en matière de conformité imposées par les gouvernements et les groupes de l'industrie partout dans le monde devraient lancer un cri d'alarme afin que l'industrie du logiciel renforce les contrôles de sécurité au niveau applicatif.

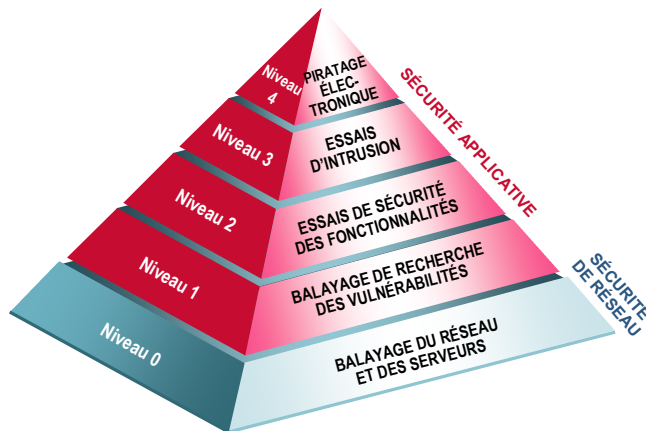
Ensemble, les équipes de développement applicatif, des opérations et d'assurance de la qualité doivent traiter la sécurité des applications d'entreprise à titre de problème de qualité et gérer la sécurité par l'intermédiaire de toutes les phases du cycle chronologique de l'élaboration des systèmes (CCES). Nous appelons cette méthode le CCES sécurisé :

CCES SÉCURISÉ DE CGI :



VOUS SENTEZ QUE VOTRE ENTREPRISE EST MAL PROTÉGÉE? LES SERVICES ASA PEUVENT VOUS DONNER UN COUP DE MAIN

La pratique d'assurance de la sécurité applicative (ASA) de CGI est dirigée par des spécialistes de la sécurité possédant la certification CISSP. On y utilise les processus et les méthodologies en matière de sécurité ayant fait leurs preuves dans l'industrie, de même qu'un large éventail d'outils commerciaux, libres et propriétaires. Notre approche progressive en matière d'essais de sécurité composée de quatre niveaux vous offre la plus haute assurance que les actifs de votre entreprise demeurent des actifs et ne deviennent pas des responsabilités.



Niveau 1 : Balayage de recherche des vulnérabilités – approche automatisée permettant de déceler les vulnérabilités connues de la plateforme causées par des logiciels dont la version est désuète, des correctifs de sécurité manquants, une mauvaise configuration de l'infrastructure et des écarts aux procédures et aux lignes directrices opérationnelles en matière de sécurité.

Niveau 2 : Essais de sécurité des fonctionnalités – vise le code et la logique applicative afin de s'assurer que les utilisateurs sont limités à des rôles fonctionnels et à des cas d'utilisation spécifiques. L'exécution des essais se fait manuellement à l'aide de jeux d'essais de mauvaise utilisation conçus au préalable.

Niveau 3 : Essais d'intrusion – permet de s'assurer que seuls les utilisateurs auxquels on a accordé accès au système sont en mesure d'accéder aux applications, et ce, uniquement par les passerelles appropriées. Les techniques avancées de piratage sont utilisées par des ressources spécialisées afin de déterminer quelles vulnérabilités de l'application sont exploitables.

Niveau 4 : Piratage électronique invisible – simule une méthode d'attaque réelle où les découvertes et les attaques se répètent et où les privilèges augmentent. Il s'agit de la forme d'essais de sécurité la plus puissante et la plus révélatrice, mais également une des plus ambitieuses au point de vue technique.

Notre engagement

CGI croit à la mise en œuvre de technologies qui transforment les environnements d'affaires de ses clients. C'est pourquoi nous offrons nos services complets aux entreprises appartenant à des secteurs d'activités ciblés que nous connaissons à fond. Cela nous permet de bien comprendre les défis concrets auxquels nos clients sont confrontés et de posséder le savoir-faire ainsi que les solutions qu'il leur faut pour réaliser leurs objectifs d'affaires.

Évaluation des risques en matière de sécurité applicative

Nous pouvons assurer une gestion efficace de la sécurité de vos applications et de l'infrastructure associée en aidant votre organisation à déceler et à atténuer les risques reliés à la sécurité.

- Évaluation des menaces et des vulnérabilités
- Analyse des risques (évaluation de l'impact, des probabilités et de la valeur de l'actif)
- Plan de gestion des risques (acceptation, refus, transfert et atténuation)

Notre équipe de spécialistes certifiés CISSP peuvent aider votre équipe de développement de logiciels :

- Élaboration d'une architecture d'application sécurisée
- Évaluation des outils et des dispositifs de sécurité applicative
- Conception de solutions de sécurité applicative

Nous offrons également les services suivants de gestion et de gouvernance relativement à la méthodologie CCES sécurisé :

- Vérification CCES sécurisé
- Formation CCES sécurisé
- Gestion des essais de sécurité