Chapitre 2
Panorama de la sécurité web

1. Introduction

Ce chapitre a pour but de mettre en lumière les aspects, outils et services ainsi que le vocabulaire utilisés dans le monde de la sécurité des applications web.

À des fins pédagogiques, il sera ici question des aspects techniques et de gouvernance préalables à la mise en pratique d'un cycle de développement sécurisé. Les différentes normes, lois, bibliothèques, analyses de code et modèles de maturité seront abordés afin de pouvoir les utiliser dans les prochains chapitres. Le but est de faire apparaître un corpus générique de la sécurité des applications web.

2. Les normes et référentiels

2.1 ISO/IEC 27034

Il existe un grand nombre de normes internationales concernant une multitude de branches métier. Les plus célèbres sont les normes ISO (*International Organization for Standardization*) qui définissent des exigences pour assurer la conformité des matériaux, processus et services dans une organisation.

Les normes les plus utilisées sont ISO/IEC 9000 pour la qualité, ISO/IEC 22000 pour la gestion de la sécurité des denrées alimentaires et ISO/IEC 50001 pour le management de l'énergie. Toutes ces normes sont créées par des comités dont les membres sont choisis par les organisations de normalisation leaders dans leur pays telles que l'AFNOR (Association française de normalisation) pour la France par exemple.

Les avantages des normes internationales sont nombreux ; elles assurent généralement le bon fonctionnement d'un service et permettent la certification des entreprises, ce qui est un gage de qualité dans certains métiers.

Parmi les normes les plus pratiquées figurent les séries ISO/IEC 27000 et ISO/IEC 31000 relatives au management de la sécurité de l'information. Sans entrer dans les détails, ces normes ont pour objectif d'améliorer la protection contre le vol, l'altération et la perte de données, et de maîtriser le risque au sein d'un système d'information. Ci-après, quelques exigences de l'ISO/IEC 27001 et 27002 :

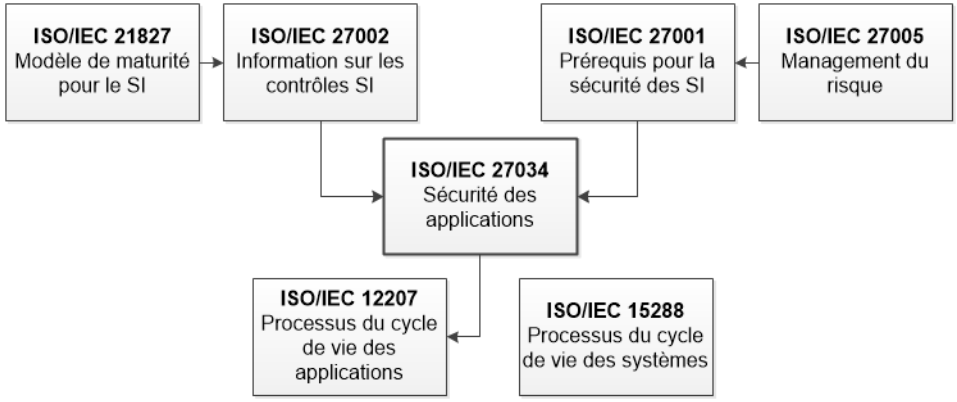
Index	Titre	Description
A.14.2.1	Politique de développement sécurisé	Des règles de développement des logiciels et des systèmes doivent être établies et appliquées au développement de l'organisation.
A.14.2.4	Restrictions relatives aux changements apportés aux progiciels	Les modifications des progiciels ne doivent pas être encouragées, doivent être limitées aux changements nécessaires et tous les changements doivent strictement être contrôlés.
A.14.2.7	Développement externalisé	L'organisation doit superviser et contrôler l'activité de développement du système externalisé.

Index	Titre	Description
A.14.2.6	Environnement de développement sécurisé	Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système.

Les items cités ci-dessus montrent bien l'intérêt d'intégrer la mise en place d'un cycle de développement sécurisé au sein des systèmes d'information des entreprises.

La norme ISO/IEC 27034 a quant à elle l'objectif d'aider les organisations à mettre en place de la sécurité de façon transparente tout au long du cycle de vie d'une application. Elle s'intègre parfaitement avec les normes ISO/IEC 27001 et ISO/IEC 27002.

Ci-dessous, la relation entre les normes ISO/IEC 27000.



Nous pouvons constater que l'ISO/IEC 27034 est une suite logique de la politique de sécurité de l'information, d'après l'organisme ISO.

Voici ce que contient la norme avec ses différents points :

Partie de la norme	Titre	Publication
ISO/IEC 27034-1:2011	Aperçu et concept de la sécurité des applications	publié
ISO/IEC 27034-2:2015	Cadre normatif d'une organisation	publié
ISO/IEC 27034-3	Processus de la sécurité d'une application	brouillon
ISO/IEC 27034-4	Validation de la sécurité d'une application	abandonnée
ISO/IEC 27034-5	Protocoles et contrôles pour la structure des données	brouillon
ISO/IEC 27034-6	Études de cas	brouillon
ISO/IEC 27034-7	Assurance pour la sécurité applicative	brouillon

Les sept parties de la norme représentent concrètement les différents points à aborder lors de la mise en place d'un cycle de développement sécurisé au sein d'une organisation. Malgré cela, l'ISO/IEC 27034 n'est pas encore suffisante car seulement deux parties sont publiées par le comité et d'autres outils abordent de façon plus pragmatique et avec plus de maturité ces mêmes sujets.

La norme est payante et accessible à cette adresse : http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378

2.2 PCI-DSS et PA-DSS

La norme PCI-DSS a été créée en 2005 par le groupe américain *Payment Card Industry Security Standards Council* (PCI SSC) et regroupe des entreprises telles que Visa, MasterCard, American Express, JCB et Discover Financial Services.

Son but est la mise en place de bonnes pratiques en matière de protection des données stockées sur les cartes bancaires pour les différents acteurs tels que les banques, commerçants, sociétés e-commerce et hébergeurs de solutions bancaires.

PCI-DSS comporte douze exigences, dont :

– Installer et gérer une configuration de pare-feu pour protéger les données du titulaire,
– Chiffrer la transmission des données du titulaire sur les réseaux publics ouverts,
– Utiliser des logiciels antivirus et les mettre à jour régulièrement,
– Restreindre l'accès physique aux données du titulaire,
– Tester régulièrement les processus et les systèmes de sécurité.

Les exigences ci-dessus montrent le pragmatisme de la PCI-DSS et couvrent bien l'essentiel des différents aspects de sécurité d'un processus de paiement à l'intérieur d'un système d'information.

Une fois ces critères remplis, le commerçant (entreprise ayant la gérance des données bancaires) peut demander par une société agréée à être audité afin d'obtenir l'accréditation PCI-DSS, qui sera valable un an.

De façon évidente, les actions requises pour l'accréditation PCI-DSS ne sont pas les mêmes suivant les profils des organisations. Il existe quatre niveaux définis par PCI concernant le type d'activité, ci-dessous un tableau récapitulatif :

Niveau	Type d'activité	Actions requises pour la conformité
1	Tout commerçant traitant plus de 6 millions de transactions Visa ou MasterCard par an. Tout commerçant ayant subi une compromission.	– Audit de sécurité sur site (ou SAQ pour Visa Europe) – Scan de vulnérabilité trimestriel (si commerce en ligne)
2	Tout commerçant traitant de 1 à 6 millions de transactions Visa ou MasterCard par an.	– Questionnaire d'autoévaluation annuel – Scan de vulnérabilité trimestriel (si commerce en ligne)

Niveau	Type d'activité	Actions requises pour la conformité
3	Tout commerçant traitant de 20 000 à 1 million de transactions Visa ou MasterCard par an.	– Questionnaire d'autoévaluation annuel – Scan de vulnérabilité trimestriel (si commerce en ligne)
4	Tout commerçant traitant moins de 20 000 transactions de commerce en ligne Visa ou MasterCard par an. Tous les autres commerçants traitant jusqu'à 1 million de transactions Visa ou MasterCard par an.	– Questionnaire d'autoévaluation annuel – Scan de vulnérabilité trimestriel recommandé (si commerce en ligne. Cela dépend de si les données sont capturées, stockées ou transmises par l'infrastructure du commerçant ou par un fournisseur de services.)

La norme PCI-DSS n'est donc pas un acquis car il est nécessaire de façon générale d'auditer le site web tous les ans tout comme il devra être effectué un scan de vulnérabilité tous les trimestres.

Le conseil PCI a pensé aussi aux concepteurs de logiciels en introduisant la norme PA-DSS (*Payment Application Data Security Standard*) qui définit les procédures et exigences d'évaluation de sécurité d'applications de paiement.

Contrairement au PCI-DSS, la PA-DSS se limite à l'application en elle-même et non pas à son environnement extérieur. La PA-DSS est issue de la PCI-DSS et donc, il n'est pas possible d'être certifié PCI-DSS avec seulement l'accréditation PA-DSS.

Pour conclure, cette norme permet aux concepteurs de logiciels d'être accrédités afin de pouvoir vendre des logiciels avec les prérequis nécessaires en sécurité pour des systèmes de paiement.