

OUTILS POUR LA GESTION DE LA SECURITE DES TECHNOLOGIES DE L'INFORMATION

FICHE 4 | NORME ISO/IEC 13335 - NORME ISO/IEC 15408

ISO/IEC 13335
ISO/IEC 15408



CONTEXTE

Les réseaux d'entreprise sont exposés à toutes sortes d'attaques informatiques qui vont du simple challenge entre hackers, aux attaques ciblées par d'autres organisations ou entreprises concurrentes en passant par le sabotage de serveurs dans le but de discréditer l'entreprise. Les attaques internes semblent aussi, en période de crise économique, en augmentation. En effet certains employés de sociétés informatiques se sentant menacés provoquent des pannes inopinées pour prouver leur utilité. Ainsi les problèmes de protection et préventions contre les attaques informatiques sont de plus en plus complexes et variés puisque :

- les entreprises sont de plus en plus délocalisées et donc disposent de réseaux intranet et extranet nationaux ou/et mondiaux,
- les attaques peuvent être externes et internes,
- les collaborateurs sont de plus en plus mobiles et donc les réseaux d'accès de plus en plus nombreux et variés.

Le résultat de cette situation est qu'une entreprise de taille moyenne désirant se protéger est confrontée à des dizaines voire centaines de dispositions internes de sécurités couvrant les aspects réseaux et applications. À ces dispositions de sécurité sont aussi souvent associées des données administratives nouvelles ou déjà existantes. Ainsi, le responsable des services informatiques et le responsable de la sécurité, doivent travailler de plus en plus en étroite collaboration pour garantir la consistance des données administratives.

À QUI S'ADRESSE CE MANAGEMENT ?

N'importe quel organisme peut appliquer la démarche de ces normes pour démontrer et valider que le produit correspondant a un niveau de sécurité suffisant. La validation peut être :

- seulement théorique (méthodes de travail, sécurité des locaux, des développements
- également physique : vérification physique (visite des locaux)

POURQUOI UTILISER DES NORMES EN GESTION DE LA SECURITE ?

Ces certifications correspondent à un avantage concurrentiel en matière de sécurité; elles ont le mérite d'être internationales. Elles ne constituent pas un but en soit. Par exemple, la norme ISO 15408 permet aux Profils de Protection utilisés d'être comparés au niveau de sécurité des différents produits envisagés dans une architecture. Dans le cadre de cette comparaison, il est donc très important de connaître ce qui se cache derrière le niveau atteint en terme de certification.

ORIGINE DES NORMES

➤ ISO 13335

L'origine de cette norme, en 1996, 4 documents (rapports techniques) considérés comme des références en matière de sécurité de l'information:

- 1) définitions et concepts de base
- 2) informations sur l'organisation à prévoir dans toute entreprise
- 3) approches de gestion du risque
- 4) guide de choix des mesures préventives selon les circonstances de l'environnement, etc.

Aujourd'hui la norme se décompose en 4 parties :

ISO 13335-1 : Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications (2004)

ISO 13335-3 : Techniques pour la gestion de sécurité IT (1998)

ISO 13335-4 : Sélection de sauvegardes (2000)

ISO 13335-5 : Guide pour la gestion de sécurité du réseau (2001)

➤ ISO 15408

Cette norme est issue d'une convergence progressive en 1996 entre les normes de l'Orange Book et de la NASA (USA) ainsi que de l'ITSEC en Europe. Elle a été baptisée critères d'évaluation de la sécurité des technologies de l'information ou critères communs. Elle se compose actuellement de 3 parties :

ISO 15408-1 : Introduction et modèle général

ISO 15408-2 : Exigences fonctionnelles de sécurité

ISO 15408-3 : Exigences d'assurance de sécurité

MISE EN ŒUVRE

ISO 15408 : La certification propose 7 niveaux d'assurance de l'évaluation - EAL (*Evaluation Assurance Level*) :

- EAL1 à EAL4 : qui correspondent à des systèmes courants de bonne qualité et à la mise en œuvre de bonnes pratiques.
- EAL5 à EAL7 : qui correspondent à des systèmes conçus avec une démarche et des méthodes de sécurisation particulièrement poussées.
- EAL7 : répond notamment à des problématiques de stratégie nationale de sécurité.

Dans le détail, les 7 niveaux sont les suivants :

- **EAL1** : testé fonctionnellement.
- **EAL2** : testé structurellement
- **EAL3** : testé et vérifié méthodiquement.
- **EAL4** : conçu, testé et vérifié méthodiquement.
- **EAL5** : conçu de façon semi-formelle et testé.
- **EAL6** : conception vérifiée de façon semi-formelle et système testé.

- **EAL7** : conception vérifiée de façon formelle et système testé.

CERTIFICATION

ISO 15408 : En France, il existe 6 CESTI (Centre d'Evaluation de la Sécurité des Technologies de l'Information), qui sont chargés de l'évaluation :

- Algoriel
- AQL (Silicomp)
- CEA LETI
- CEACI
- Oppida
- Sema technologies

En dernière instance, c'est la DCSSI qui valide l'agrément et délivre le certificat.

DEGRÉ D'APPLICABILITÉ

Normes – outils pour la gestion de la sécurité : où en êtes-vous ?

Nom et version	Description	Applicabilité/portée	Spécification	Évolution
ISO 13335				
13335 – 1	Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications	Immédiate/internationale	Publiée en 2004	Stable
13335 – 3	Techniques pour la gestion de sécurité IT	Immédiate/internationale	Publiée en 1998	Stable
13335 – 4	Sélection de sauvegardes	Immédiate/internationale	Publiée en 2000	Stable
13335 – 5	Guide pour la gestion de sécurité du réseau	Immédiate/internationale	En révision	Stable
ISO 15408				
15408 – 1	Introduction et modèle général	Immédiate/internationale	Publiée en 2005	Stable
15408 – 2	Exigences fonctionnelles de sécurité	Immédiate/internationale	Publiée en 2005	Stable
15408 – 3	Exigences d'assurance de sécurité	Immédiate/internationale	Publiée en 2005	Stable