SARSSI 2013 - Mont de Marsan

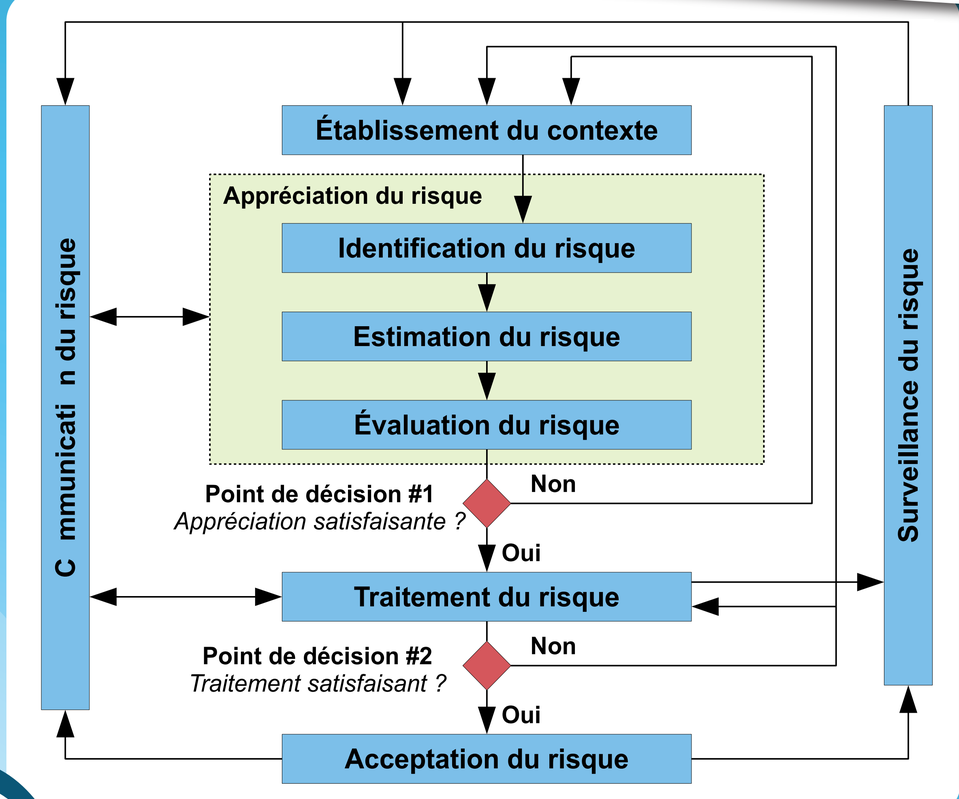
Gestion des Risques

dans les Systèmes d'Information Orientés Services

Vincent Lalanne - Manuel Munier - Alban Gabillon

Résumé : Les architectures orientées services (SOA) offrent de nouvelles possibilités pour l'interconnexion des systèmes d'information. L'ouverture du SI d'une entreprise sur l'extérieur n'est toutefois pas anodine du point de vue de la sécurité. Que ce soit pour utiliser des services proposés par des tiers ou pour offrir les siens, ces technologies introduisent de nouvelles vulnérabilités dans le SI et, par conséquent, de nouveaux risques. Nos travaux visent à initier une démarche de gestion de ces risques qui s'appuie sur un standard, la norme ISO/IEC 27005:2011. Nous proposons une évolution de cette norme afin qu'elle puisse prendre en compte pleinement le type « service ». Suite à cette étude nous introduisons également un nouveau critère, la maîtrisabilité, pour qualifier la sécurité des systèmes d'informations.

ISO/IEC 27005:2011



Un monde de services

L'interconnexion des systèmes d'information, avec en particulier le développement des architectures orientées services (SOA), permet la création de nouveaux services par la composition (orchestration, chorégraphie) de services existants sur Internet.

Il n'est plus possible, à l'heure actuelle, de dissocier les services web d'un autre concept qui leur est proche : le « cloud » : ce concept fait appel à de nombreux services dans le domaine du traitement, du stockage, de la transformation de l'information.

La notion de « service » soit être prise en compte dans le processus de gestion des risques au niveau de la sécurité de l'information.

Notion de Maîtrisabilité

La qualité de service : il n'est pas rare d'être confronté à des pannes fréquentes, les services deviennent indisponibles, ce qui peut toucher des milliers d'utilisateurs de par le monde. La seule compensation possible est d'ordre financière alors que votre image a été lourdement dégradée.

La localisation des données et des traitements : ces services externalisés peuvent être situés dans le monde entier, sans qu'il soit possible de pouvoir choisir le pays. Dans la plupart des cas, le prestataire de cloud ignore lui-même où sont les données et où sont exécutés les traitements de l'information .

La perte de contrôle de l'information dont l'origine peut avoir des causes bien différentes. En cas d'incident chez le prestataire de services, est-il toujours possible de récupérer ses données ? Est-ce aux clients ou au fournisseur de services de faire des sauvegardes ? De plus qu'en est-il de la réversabilité qui est censée permettre au client de reprendre possession de ses données, à tout moment, sans justification ?

La propriété de l'information : quand on traite des informations dans le cloud, on confie le capital de l'entreprise à un tiers. Que se passe-t-il en cas de litige (ex : non-paiement, injonction), s'il cesse son activité (ex : faillite, rachat),. . . ? Le prestataire a-t-il la possibilité de garder vos données? A-t-il contractuellement le droit de les exploiter ?

Dans tous les cas l'architecte doit garder la maîtrise de ses services !

Vulnérabilités liées aux services

Type	Exemples de vulnérabilités	Exemples de menaces
Matériel	. . .	. . .
Logiciel	. . .	. . .
Réseau	. . .	. . .
Service	Pas de support à long terme du fournisseur de service	Le service n'est plus disponible
	Le cycle de vie et les politiques de mise à jour du fournisseur de service sont inconnus	Changement inattendu de l'interface du service
	Hébergement des services dans un pays inconnu	Espionnage, vol de données
	Ne se conforme pas avec les lois en vigueur	Le service n'est plus disponible
	Le fournisseur fait faillite	Le service n'est plus disponible
	Les lois sur la vie privée du pays d'hébergement sont différentes des lois du pays d'utilisation de ces données	Perte de confidentialité
	Permissivité des lois sur la sécurité de l'information	Espionnage, vol de données
	Sévérité des lois sur la sécurité de l'information sont	Le service n'est plus disponible
	Contrat de niveau de service inapproprié	Perte de maitrisabilité du SI
	Pas de procédure de récupération des données	Perte de maitrisabilité du SI
	Manque de réversibilité (migration, interopérabilité)	Perte de maitrisabilité du SI
	Absence de procédure d'effacement des données à la fin du contrat	Vol de données, utilisation non autorisée
	Absence de sécurisation des métadonnées du WS	Falsification du web service
	Possibilité d'appels multiples du WS	Usurpation d'identité
	Absence de traçabilité du service fourni	Absence de confiance dans l'information
Personnel	. . .	. . .
Site	. . .	. . .
Organisation	. . .	. . .

Table : Un nouveau type "service" dans l'annexe D de la norme ISO/IEC 27005:2011

ALBAN GABILLON
alban.gabillon@upf.pf
Université de Polynésie Française
GePaSud EA 4238

VINCENT LALANNE
vincent.lalanne@univ-pau.fr
MANUEL MUNIER
manuel.munier@univ-pau.fr
Université de Pau et des Pays de l'Adour
LIUPPA EA 3000