|  |  |  |
| --- | --- | --- |
| logo | Applications | 1085 |

Responsable :

Mis à jour :

Les exigences en matière de sécurité de l'information sont identifiées, spécifiées, traitées et approuvées lors du développement ou de l'acquisition d'applications.

Les exigences de sécurité des applications sont généralement déterminées par une évaluation des risques et couvrent un large éventail de sujets.

Les exigences de sécurité des applications incluent, selon le cas :

* le niveau de confiance dans l'identité des entités
* l’identification du type de l'information et le niveau de classification à traiter par l'application
* le besoin de séparation de l'accès et du niveau d'accès aux données et fonctions dans l'application
* la résilience contre les attaques malveillantes ou les interruptions involontaires (protection contre les débordements de tampon ou les injections SQL - langage de requête structuré)
* les exigences légales, statutaires et réglementaires de la juridiction où la transaction est générée, traitée, complétée ou stockée
* le besoin de confidentialité associé à toutes les parties impliquées
* les exigences de protection de toute information confidentielle
* la protection des données en cours de traitement, en transit et au repos
* la nécessité de crypter en toute sécurité les communications entre toutes les parties concernées
* le contrôle des entrées, y compris les contrôles d'intégrité et la validation des entrées
* les contrôles automatisés (limites d'approbation ou doubles approbations)
* les contrôles de sortie (qui peut accéder aux sorties et qui donne son autorisation)
* les restrictions concernant le contenu des champs « en texte libre », car cela peut conduire à un stockage incontrôlé de données confidentielles personnelles
* les exigences dérivées du processus métier, telles que la journalisation et la surveillance des transactions, les exigences de non-répudiation
* les exigences imposées par d'autres mesures de sécurité (interfaces avec la journalisation et la surveillance ou les systèmes de détection des fuites de données)
* la gestion des messages d'erreur

Pour les applications offrant des services transactionnels entre l'organisation et un partenaire, les éléments suivants sont pris en compte lors de l'identification des exigences de sécurité de l'information :

* le niveau de confiance que chaque partie exige dans l'identité revendiquée de l'autre
* le niveau de confiance requis dans l'intégrité de l’information échangée ou traitée et les mécanismes d'identification du manque d'intégrité (contrôle de redondance cyclique, hachage, signatures numériques)
* les processus d'autorisation associés à qui peut approuver le contenu, émettre ou signer des documents transactionnels clés
* la confidentialité, l'intégrité, la preuve de l'envoi et de la réception des documents clés et la non-répudiation (contrats associés aux processus d'appel d'offres et de contrat)
* la confidentialité et l'intégrité de toutes les transactions (commandes, détails de l'adresse de livraison et confirmation des reçus)
* les exigences relatives à la durée de confidentialité d'une transaction
* les assurances et autres exigences contractuelles

Pour les applications impliquant une commande et un paiement électroniques, les éléments suivants sont pris en compte :

* les exigences de maintien de la confidentialité et de l'intégrité de l’information de commande
* le degré de vérification approprié de l’information de paiement fournie par un client
* la perte ou la duplication des informations de transaction
* le stockage les détails de la transaction en dehors de tout environnement accessible au public (plate-forme de stockage existant sur l'intranet de l'organisation, et non conservés et exposés sur des supports de stockage électroniques directement accessibles depuis Internet)
* la sécurité intégrée tout au long du processus de gestion des certificats ou des signatures de bout en bout lorsqu'une autorité de confiance est utilisée

Plusieurs des considérations ci-dessus peuvent être traitées par l'application de la cryptographie, en tenant compte des exigences légales.

Les applications accessibles via les réseaux sont soumises à une série de menaces liées au réseau :

* les activités frauduleuses
* les litiges contractuels
* la divulgation d'informations au public
* la transmission incomplète
* l’erreur d'acheminement
* la modification non autorisée des messages
* la duplication
* la relecture

Les contrôles requis incluent souvent des méthodes cryptographiques pour l'authentification et la sécurisation du transfert de données.