Zeitschrift: Vermessung, Photogrammetrie, Kulturtechnik : VPK = Mensuration, photogrammétrie, génie rural

Herausgeber: Schweizerischer Verein für Vermessung und Kulturtechnik (SVVK) = Société suisse des mensurations et améliorations foncières (SSMAF)

Band: 88 (1990)

Heft: 8

Artikel: La sécurité des données vue par un responsable de centre informatique

Autor: Simos-Rapin, B.

DOI: https://doi.org/10.5169/seals-234344

La sécurité des données vue par un responsable de centre informatique

B. Simos-Rapin

La sécurité informatique est un sujet d'actualité, de nombreux livres traitant de ce sujet ont paru et les grandes firmes de consultance sont toujours plus nombreuses à proposer des séminaires de formation sur ce thème.
Comment évaluer la sécurité dans l'entreprise, quels sont les risques courus et quels moyens faut-il mettre en œuvre améliorer la sécurité? L'objectif de cet article est de sensibiliser le lecteur à l'importance de ces problèmes et de lui présenter les grands axes d'une méthode de sécurité informatique, la méthode MARION.

Die Sicherheit in der Informatik ist ein sehr aktuelles Thema. In letzter Zeit wurden zahlreiche Publikationen auf diesem Gebiet veröffentlicht. Die grossen Beratungsfirmen werden immer zahlreicher, die diesbezüglich Weiterbildungsseminare anbieten.
Wie kann man die Sicherheit im Betrieb beurteilen? Welches sind die Risiken? Was muss unternommen werden, um die Sicherheit zu erhöhen? Ziel dieses Beitrages ist, die Leser für die Bedeutung der Probleme zu sensibilisieren und die Grundideen einer Methode für die Sicherheit in der Informatik, die Methode MARION, zu beschreiben.

1. Introduction

Cette dernière décennie a vu l'introduction du traitement informatique des données à grande échelle. La multiplication des matériels et des logiciels a permis de répondre à un volume sans cesse croissant de besoins tant dans les domaines administratifs que techniques tels que ceux exprimés par la mensuration et la gestion du territoire. Le recours aux moyens informatiques devient toujours plus vital pour l'entreprise. L'informatique lui permet non seulement d'en assurer son fonctionnement, mais également d'offrir à sa clientèle des biens et des services.
La dépendance de l'entreprise vis à vis de l'informatique devient telle qu'il n'est plus possible de recourir à des techniques traditionnelles en cas de non fonctionnement du système informatique. L'interruption dans l'exploitation ou les dysfonctionnements des systèmes informatiques ont des répercussions toujours plus graves pour l'entreprise et peuvent même mettre en péril sa survie.
Les données gérées par les systèmes sont un capital qu'il convient de préserver et de bien gérer.
Un plan de sécurité bien défini et appliqué permet par des mesures de prévention, protection et détection, de limiter les risques de sinistre et d'en rendre les conséquences supportables pour l'entreprise.

2. Définition

La sécurité informatique vise à réduire les risques de pertes, détournement, destruction, altération, falsification de matériel, ressources et données informatiques. Elle s'obtient par l'application d'un ensemble de mesures organisationnelles et techniques.
La sécurité informatique peut être chiffrée et améliorée grâce à l'application d'une méthode telle que la méthode MARION.

3. Types de risques

Les risques informatiques se répartissent dans les catégories suivantes:

- risques matériels
- vol et sabotage de matériel
- pannes et dysfonctionnement de matériel ou de logiciel de base
- erreurs de saisie transmission et utilisation des informations
- erreurs d'exploitation
- erreurs de conception et de réalisation
- fraude, sabotage immatériel
- indiscrétion, détournement d'information
- détournement de logiciel
- départ de personnel stratégique.

3.1 Risques matériel

Les risques matériels peuvent entraîner la destruction partielle ou totale des matériels informatiques, des supports de données et de l'environnement d'exploitation (salle informatique, salle des terminaux, etc.).
Ils peuvent survenir à la suite d'événements tels que:

- incendie, implosion, explosion
- chocs, collisions, chutes
- introduction de corps étrangers
- bris
- conséquence d'événements naturels tels qu'inondations, foudre, etc.

3.2 Vol et sabotage de matériel

Le vol concerne avant tous les matériels tels que micro-ordinateurs, périphériques et fournitures.
Le sabotage peut revêtir toutes sortes de formes et vise à paralyser le fonctionnement de l'ordinateur ou de ses périphériques. Cela peut aller du déversement de liquide sur l'unité CPU jusqu'à l'introduction d'une bombe dans les locaux informatiques.

3.3 Pannes et dysfonctionnement de matériel ou logiciel de base

Soit le matériel, soit le logiciel de base (système d'exploitation, langages, logiciel de télécommunication) peuvent présenter des pannes ou des dysfonctionnement ayant pour conséquence l'arrêt du système ou son exploitation en mode dégradé.

3.4 Erreurs de saisie, transmission et utilisation des informations

Le personnel affecté à la saisie des données peut commettre des erreurs, ce taux d'erreur, même après vérification peut être de l'ordre de 0,5%. Il s'agit d'erreur de transcription, de lecture ou encore d'interprétation des informations ou d'application des règles.
Ces erreurs ont pour conséquence une perte de temps nécessitée par leur recherche et leur correction.

3.5 Erreurs d'exploitation

Ces erreurs sont consécutives à une mauvaise manipulation de la part du personnel d'exploitation ou de l'utilisateur. Elles peuvent avoir des formes très variées telles que:

- écrasement d'un fichier ou d'une sauvegarde
- erreur due au média
- activation d'une mauvaise version d'un logiciel
- erreur dans l'interprétation d'une instruction
- mauvaise manipulation du matériel
- oubli d'une opération dans une chaîne de traitement.

Il faut relever que ces erreurs peuvent tout aussi bien provenir d'une négligence, d'un comportement laxiste ou tout simplement d'une malveillance auquel cas on parlera de sabotage immatériel.

3.6 Erreurs de conception et de réalisation

Il faut distinguer deux types d'erreurs dont les conséquences sont très différentes. Les erreurs de conception de l'application peuvent avoir de graves conséquences sur la conformité des traitements réalisés ou sur les performances du produit. Des erreurs de réalisation peuvent être plus facilement corrigées et sont en principes moins graves car elles ne remettent pas en cause l'exactitude du cahier des charges de l'application ou les options prises.

3.7 Fraude et sabotage immatériel

La fraude informatique présente souvent peu de danger pour son auteur, elle revêt plusieurs formes parmi lesquelles on peut citer:

- détournement de ressources informatiques
- détournement de biens (vol sur stock suivi d'un ajustement informatique)
- falsifications.

Le sabotage immatériel consiste à placer une bombe logique ou virus de manière à perturber ou paralyser le fonctionnement du logiciel système, des utilitaires ou des logiciels d'application.

3.8 Indiscrétion, détournement d'informations

L'indiscrétion et le détournement d'informations se révèleront être toujours plus problématiques avec l'augmentation de l'informatisation des divers secteurs d'activité.

3.9 Détournement de logiciels

Cette opération consiste en la réalisation d'une copie d'un logiciel. Il en résulte une perte qui peut se traduire en une diminution des ventes du logiciel ou en l'émergence d'une concurrence.

3.10 Départ de personnel stratégique

Le départ de personnel de développement ou d'exploitation très spécialisé entraîne une perte importante pour l'entreprise. Il peut être dû la mauvaise qualité des relations dans l'entreprise ou consécutif au non règlement d'un conflit.

4. Types de pertes

Les types de pertes peuvent se résumer comme suit:

- dommages matériels et annexes
- frais supplémentaires
- pertes d'exploitation
- pertes de fonds
- autres pertes.

4.1 Dommages matériels et annexes

Ces pertes comprennent le coût de remplacement des matériels endommagés, détruits ou volés. Ils concernent également la remise en état du matériel d'environnement tels que locaux, installations électriques, installation de climatisation, etc.

4.2 Frais supplémentaires

Ce sont les frais résultant de la mise en œuvre de moyens de secours tels que:

- ressources informatiques et télématiques
- matériel d'environnement
- personnel informatique et non-informatique supplémentaire
- primes spéciales
- frais de transport du matériel
- location de matériel et de locaux
- frais d'étude et de réalisation pour la remise à niveau des données et des logiciels
- frais de reconstitution des données.

4.3 Pertes d'exploitation

Les pertes d'exploitation résultent des effets du non fonctionnement ou d'un fonctionnement partiel du système pendant la période de reconstruction.

Elles peuvent recouvrir des:

- pertes d'intérêts bancaires
- pertes de chiffre d'affaire
- pertes de clientèle.

4.4 Pertes de fonds

Ce sont des pertes de biens fianciers tels que pertes de chèques ou de virements.

4.5 Pertes de biens

Les pertes de biens correspondent à la disparition de biens matériels en stock, non encore stockés ou immobilisés.

4.6 Autres pertes

Ce peuvent être des frais de justice, des frais d'expertise, etc.

5. Répartition des sinistres

L'association française APSAIRD (Assemblée Plénière des Sociétés d'Assurances contre l'Incendie et les Risques Divers) répertorie depuis quelques années les sinistres que lui annoncent les compagnies d'assurance, les associations professionnelles ou les victimes. Ces données sont complétées par des enquêtes réalisées par divers organismes.
Même si les chiffres de la littérature ne correspondent pas tout à fait à la réalité, ils permettent de se faire une idée de la répartition des sinistres par type de risque.

14,5	%	:	risques matériels
1	%	:	vol et sabotage de matériel
15	%	:	pannes et dysfonctionnement de matériel ou de logiciel de base
19	%	:	erreurs de saisie, transmission et utilisation des informations
6	%	:	erreurs d'exploitation
9	%	:	erreurs de conception et de réalisation
17,5	%	:	fraude, sabotage immatériel
3	%	:	indiscrétion, détournement d'information
12,5	%	:	détournement de logiciel
1,5	%	:	départ de personnel stratégique
1	%	:	divers

En regroupant ces risques on obtient les catégories suivantes:

30,5	%	:	risques accidentels
34	%	:	erreurs
33	%	:	actions malveillantes
2,5	%	:	autres

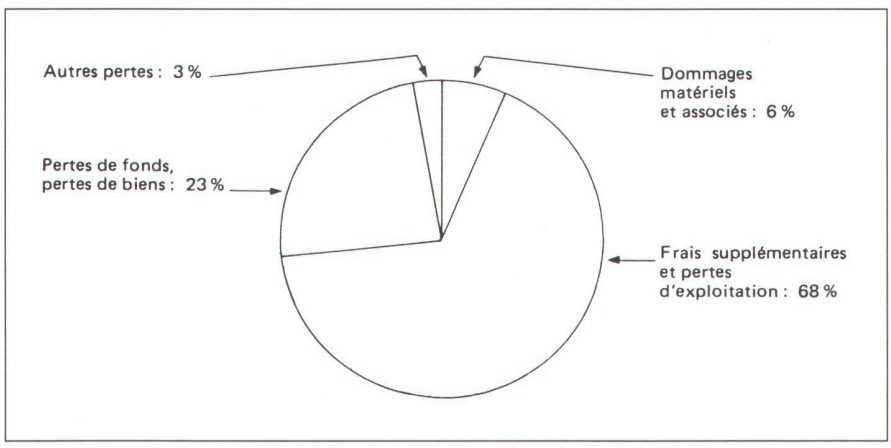

Fig. 1: Répartition des sinistres par type de perte (données de 1984) [2].

En répartissant les sinistres par type de perte, on obtient les pourcentages suivants:

6	% :	dommages matériels
68	% :	frais supplémentaires et pertes d'exploitation
23	% :	pertes de fonds et pertes de biens
3	% :	autres pertes

On remarque que les risques se répartissent pour une part égale en risques accidentels, erreurs et actions malveillantes alors que les pertes subies par les frais engagés pour la reconstitution des données, location de matériel, engagement de personnel et les pertes d'exploitation dipassent largement celles dues à la perte même totale du matériel.

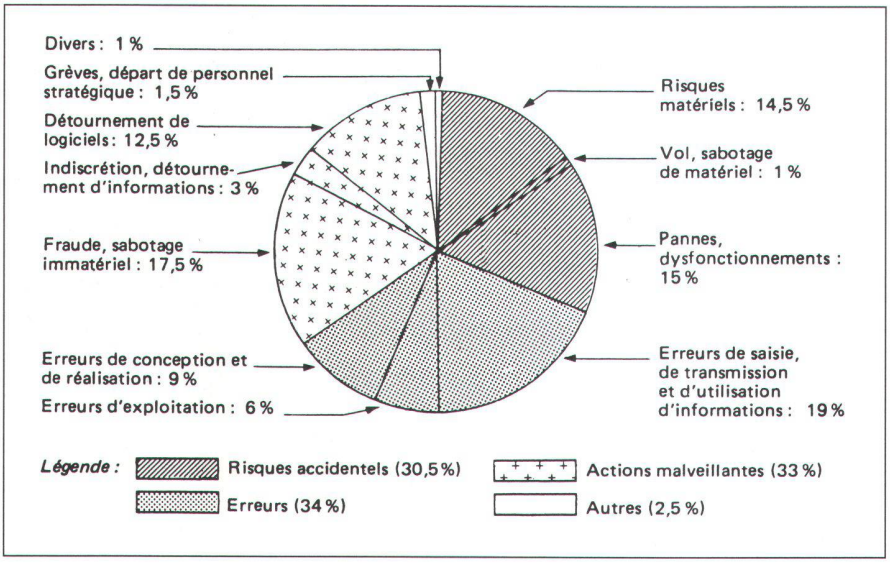

Fig. 2: Répartition des sinistres par type de risque (données de 1984) [2].

6. Méthodologie d'évaluation des risques – la méthode MARION

Il existe plusieurs méthodes d'évaluation des risques informatiques et d'aide à l'élaboration de solutions ayant pour but de rendre ces risques acceptables pour l'entreprise. Le Club de la Sécurité Informatique Français (CLUSIF) a créé des méthodes qui sont déjà bien répandues telles que MARION-AP et MARION-SRX. Pour répondre plus spécifiquement aux besoins des PME, l'APSAIRD en collaboration avec le CLUSIF, a mis au point la méthode MARION-PME.

La méthode comprend deux volets, l'analyse de la situation et la proposition d'un plan d'orientation.

L'analyse de la situation doit permettre de faire le point sur la sécurité dans l'entreprise alors que la plan d'orientation, destiné à la direction, propose l'application d'un ensemble de mesures.

Les deux volets recouvrent six étapes qui ont pour objectif de répondre aux questions suivantes:

- quels risques court-on? (étape no 1)
- peut-on accepter risques (étape no 2)
- quelle est la qualité de la sécurité actuelle (étape no 3)
- quelles sont les contraintes (étape no 4)
- comment améliorer de manière cohérente la sécurité (étape no 5)
- quel plan d'action à mettre en œuvre (étape no 6).

6.1 Etape no 1: Analyse des risques

Cette étape permet de déterminer les risques encourus par l'entreprise et dus à l'informatique.

6.2 Etape no 2: Expression du risque maximum admissible

La capacité de l'entreprise est établie sur la base d'analyses financières. Elle consiste à exprimer le risque maximum admissible, donc la perte maximale que peut subir l'entreprise du fait des événements redoutés sans mettre en péril sa survie.

6.3 Etape no 3: Analyse des moyens de la sécurité

L'analyse des moyens de la sécurité permet de chiffrer la qualité des mesures actuelles mises en œuvre pour assurer la sécurité. Cette analyse est effectuée à l'aide de questionnaires; les réponses sont pondérées par des poids établis sur la base des sinistres observés. Il est alors possible de faire apparaître les incohérences des moyens actuels de la sécurité face aux risques.

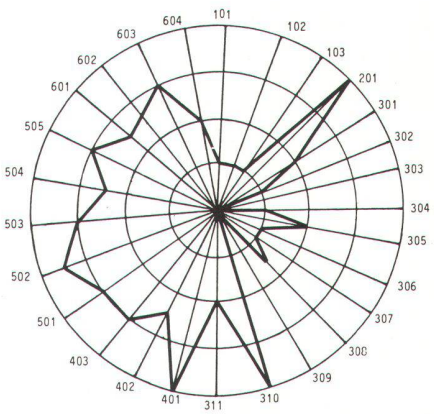

Fig. 3: Rosace de synthèse de l'analyse de la sécurité [2].

Les principaux points évalués se répartissent en cinq domaines et regroupent vingt-sept facteurs de sécurité.

Ces domaines sont:

- l'environnement organisationnel et économique
- la sécurité physique
- la sécurité informatique de base
- la sécurité d'exploitation
- la sécurité des applications.

6.4 Etape no 4: Définition des contraintes

Cette étape doit permettre d'analyser et de discuter les contraintes techniques et financières. Elle permet de fixer quelle est la part minimale du budget supplémentaire de la sécurité que l'on doit imputer à la prévention afin de minimiser le coût des sinistres.

6.5 Etape no 5: Choix des moyens

L'objectif de cette étape est de préciser les moyens de sécurité sur lesquels il est prioritairement nécessaire d'intervenir. On distingue les moyens de protection, permettant de réduire le risque maximum en dessous de la capacité de l'entreprise et les moyens de prévention permettant d'abaisser le coût moyen des risques.

Il est tenu compte, dans le choix des moyens, des priorités fixées ainsi que des contraintes définies dans l'étape no 4 (Définition des contraintes).

6.6 Etape no 6: Plan d'orientation

Lors de cette étape, on détaille les solutions évoquées dans l'étape précédente et on examine dans quelle mesure les orientations proposées réduisent suffisamment les risques. Si nécessaire on prend la décision d'opérer un transfert de risque par la conclusion d'une assurance.

Le plan d'orientation rédigé contient le détail des solutions techniques retenues, leur coût et le planning de réalisation.

7. Présentation de quelques points de la méthode

7.1 Etape no 3: Analyse des moyens de la sécurité

7.1.1 L'environnement organisationnel et économique

Sont évalués la qualité et l'existence:
de mesures de types organisationnelles prises par l'entreprise telles que:

- réunions périodiques de la direction et des responsables de la sécurité
- information du personnel sur les problèmes de sécurité
- existence d'un organigramme des tâches par poste
- existence de contrats d'assurances couvrant les risques informatiques

de contrôles permanent tels que:

- existence de procédures écrites permettant à l'utilisateur de contrôler les informations à la réception, à la saisie, au traitement et à l'archivage des informations
- existence d'un correspondant informatique par fonction informatisée

d'une réglementation indiquant:

- archivage et classement fiable des documents originaux afin de permettre une reconstitution ou une utilisation rapide de l'information.

7.1.2 La sécurité physique

Elle porte sur les points suivants:

l'environnement de base:

- existence d'une étude, mise périodiquement à jour, portant sur les dangers présentés par un éventuel dégât d'eau et la sécurité de la construction
- vérification périodique de la qualité de l'alimentation électrique des installations électriques liées à l'informatique
- protection du bâtiment et des locaux de l'informatique contre la foudre

les contrôles d'accès:

- contrôle d'accès aux bâtiments et contrôle d'accès sélectifs aux locaux informatiques

la pollution:

- impression dans un local distinct de l'ordinateur
- dépoussiérage périodique des locaux informatiques
- maintenance des installations de climatisation (changement des filtres)
- revêtement de sol anti-statique

les consignes de sécurité:

- existence de consignes liées au risques informatiques
- sensibilisation, information et formation du personnel
- réalisation de tests impromptus

la sécurité incendie:

- existence de poubelles anti-feu dans la salle ordinateur
- existence de meubles anti-feu pour le stockage des documents, copies de sécurités et copies de données stratégiques
- existence d'extincteurs mobiles
- existence d'installation d'extinction automatique dans les salles ordinateur
- sensibilisation, formation et information du personnel

la sécurité dégâts des eaux:

- localisation des blocs de climatisation hors de la salle ordinateur
- existence d'un système d'évacuation des eaux
- présence de détecteurs d'eau dans les faux-planchers

la fiabilité de fonctionnement des matériels informatiques:

- existence d'un système de climatisation
- existence d'un système d'amélioration et de stabilisation de la qualité de l'alimentation électrique
- vérification et maintenance périodique des installations techniques.

7.1.3 La sécurité informatique générale

Elle prend en compte:
les systèmes et procédures de secours:

- existence d'un plan de secours remis à jour périodiquement
- existence d'un système de secours: en interne ou en externe (système de back-up, télébackup, salle blanche, systèmes identiques répartis)
- test des solutions de secours en réel (au moins deux fois par an)

les protocoles de relation utilisateurs-informatique:

- existence d'un comité de direction étudiant régulièrement les problèmes liés à l'informatique
- assistance, encadrement et suivi des utilisateurs pour le choix de moyens autonomes ou de progiciels

le personnel informatique:

- formation externe du personnel informatique au moins 5 jours par an
- formation et information du personnel sur les problèmes de sécurité
- règlement écrit sur les obligations et responsabilités du personnel concernant l'utilisation, la conservation et l'archivage d'information indépendamment du type de support

les plans informatiques et de sécurité:

- existence d'un plan informatique
- existence d'un plan de sécurité
- validation et suivi de ces plans par un comité

la sécurité offerte par le matériel et le logiciel de base:

- système récent et courant (matériel et logiciels)
- existence d'un système de contrôle des accès logiques aux ressources
- existence d'outils de contrôle et de suivi des accès aux ressources

la sécurité des télécommunications:

- matériel de télécommunication et têtes de lignes dans des locaux isolés et protégés
- identification et authentification des utilisateurs par mot de passe

la protection des données:

- désignation d'un responsable pour la mise en place, la surveillance et la modification des fichiers et bases de données
- existence d'outils de contrôle de l'intégrité des données
- affectation des droits d'accès en fonction du degré stratégique des informations
- journalisation des mises à jour.

7.1.4 La sécurité de l'exploitation

l'archivage et le désarchivage:

- procédures écrites concernant le stockage et l'utilisation des supports d'archives informatiques
- stockage des supports dans un local d'archives physiquement séparé de la salle d'ordinateur
- procédure de mise à disposition et d'utilisation des supports

la saisie et le transfert classique des données:

- procédure de contrôle des documents par les utilisateurs, avant la saisie
- procédure de transfert des données stratégiques dans des conteneurs sécurisés par des convoyeurs accrédités

la sauvegarde:

- existence d'une sauvegarde systématique stockée dans des locaux protégés et physiquement distincts des locaux informatiques
- existence d'au moins une génération de sauvegarde stockée à l'extérieur de l'entreprise
- tests périodique de la restauration des supports de sauvegarde
- stockage d'une copie de la documentation technique dans des locaux protégés externes à l'entreprise

le suivi de l'exploitation:

- séparation des environnements développement et production et contrôle des transferts entre ces deux environnements

- existence d'une documentation d'exploitation complète, tenue à jour et stockée dans un lieu protégé

la maintenance:

- existence de contrats de maintenance pour tous les matériels informatiques, les matériels d'environnement et les logiciels de base
- existence d'un centre de support téléphonique
- existence d'un carnet de maintenance propriété de l'entreprise.

7.1.5 La sécurité des applications

les protocoles de recette:

- existence d'un protocole de recette pour toute mise en exploitation d'une application nouvelle ou d'une maintenance
- conception de jeux d'essai par les utilisateurs
- existence d'un dossier utilisateurs pour chaque nouvelle application

les méthodes d'analyse-programmation:

- existence d'un avant-projet et d'un cahier des charges pour chaque nouveau projet
- planification des projets en développement ou en maintenance
- utilisation d'une méthodologie d'analyse fonctionnelle et de programmation formalisée et normalisée

les contrôles programmés:

- contrôle des données fonction de leur importance stratégique
- mise en place de différents types de contrôles tels que vraisemblance et cohérence

la sécurité des progiciels:

- étude comparative de produits avant le choix de progiciels
- prise en compte de la capacité des sociétés de services à maintenir et faire évoluer les produits
- clause contractuelle permettant l'obtention des programmes sources en cas de défaillance de la société de service
- clause contractuelle de fourniture d'une documentation complète et d'une formation de base.

8. La sécurité dans un centre informatique de petite dimension

8.1 Un exemple d'application

L'exemple présenté met en évidence les normes de sécurité appliquées dans un centre informatique pour ingénieurs géomètres.

8.2 Contexte

8.2.1 Matériel

Un ordinateur central dessert en interne, 5 terminaux, une station graphique et un plotter.
Quatre lignes téléphoniques louées à 9600 bauds permettent aux quatre bureaux d'ingénieurs géomètres, partenaires du centre, d'activer toutes les applications classiques de calcul, de faire des impressions et des restitutions sur leur site.
Une ligne louée à 56 kilobaud permet d'interroger les bases de données de la Direction du Cadastre et de rapatrier sur la machine du centre les données souhaitées.
La machine du centre et celle de la Direction du Cadastre fonctionnent avec le même système d'exploitation; elles sont toutes deux connectées en réseau.

8.2.2 Personnel

Le centre emploie trois ingénieurs et une secrétaire.
Deux ingénieurs se partagent les tâches d'exploitation, de développement et de formation, le troisième assume des tâches administratives et de direction. En cas de besoin, il peut également assurer des tâches d'exploitation et de formation.
Un ingénieur est responsable du fonctionnement de l'ordinateur central et des télécommunications, réalise les sauvetages, archivages et désarchivage. Un deuxième ingénieur assure les permanences.
Deux utilisateurs formés réalisent, si besoin est, les sauvetages.
Chaque domaine d'application a un responsable pour l'installation, la maintenance et le développement des produits. Un recouvrement est fait entre les domaines de façon à pouvoir assurer les transferts de connaissances et les permanences.

8.3 L'environnement organisationnel et économique

Les mesures prises sont:

- établissement de la répartition des domaines de responsabilité et des domaines d'activité
- conclusion d'une assurance couvrant les risques informatiques. Cette assurance prévoit un montant pour la restauration des données et couvre une partie des pertes d'exploitation
- contrôle des informations à la saisie et au traitement par les techniciens des bureaux.

Il n'y a pas de réunions formelles pour sensibiliser le personnel aux problèmes de sécurité.

8.4 La sécurité physique

Les facteurs de sécurité appliquées sont:

- existence d'une climatisation
- existence d'extincteurs mobiles
- impression dans un local distinct de celui de l'ordinateur
- maintenance périodique de l'installation de climatisation.

Vu la dimension du centre, il n'existe pas de restriction physique d'accès au local informatique, cependant des consignes ont été données aux employés des bureaux. Il n'y a pas d'équipement de stabilisation de l'alimentation électrique, ni de protection des locaux contre la foudre et les dégats d'eau, par contre l'ordinateur est alimenté par une ligne qui lui est propre.

8.5 La sécurité informatique générale

Les normes prises en compte sont:

- existence d'un groupe de travail étudiant les problèmes liés à l'informatique
- assistance, encadrement et suivi des utilisateurs pour le choix de moyens autonomes ou de progiciels
- formation externe du personnel informatique au moins 5 jours par an
- utilisation d'un système informatique (matériel et logiciel de base) récent et courant
- existence d'un système de contrôle des accès logiques aux ressources
- restriction d'accès par télécommunication et authentification par mot de passe
- restriction d'accès aux données par groupe d'utilisateurs.

La protection des données sur les ordinateurs personnels est réalisée grâce à un logiciel (Fileguard) dont le paramétrage permet de restreindre l'accès des utilisateurs aux données et d'empêcher le détournement de logiciels.
Un plan général de sécurité n'a pas été établi et un test d'une solution de secours n'a pas été, à ce jour, réalisé.

8.6 La sécurité d'exploitation

Les mesures de sécurité appliquées sont:

- existence d'une sauvegarde généralisée stockée dans des locaux externes à l'entreprise
- archivage et désarchivage automatisé des données selon liste fournie par les utilisateurs
- stockage décentralisé de l'original et d'une copie des données archivées
- séparation des environnements de production et de développement
- contrôle des transferts d'application entre l'environnement de développement et l'environnement de production
- existence de contrats de maintenance pour tous les matériels informatiques, les matériels d'environnement, les logiciels de base et certains logiciels d'application

- existence d'un centre de support téléphonique pour le logiciel de base

Le plan sauvetage des données est conçu de la façon suivante:

- chaque jour, sauvegarde des fichiers mutés depuis le jour précédent
- chaque semaine, sauvegarde des fichiers mutés depuis la semaine précécente
- chaque mois, sauvegarde totale.

Les sauvetages hebdomadaires et mensuels sont conservés sur une période de trois mois.
Le sauvetage des données gérées sur les ordinateurs personnels est effectué par chaque utilisateur responsable de ses données et de ses applications.
La documentation concernant les développements est insuffisante.

8.7 La sécurité des applications

Les normes appliquées sont les suivantes:

- existence d'un avant-projet et d'un cahier des charges pour chaque nouveau projet
- mise en place de contrôles de vraisemblance et de cohérence des données
- étude comparative de produits avant le choix de progiciels
- prise en compte de la capacité des sociétés de services à maintenir et à faire évoluer les produits.

Il n'y a pas, pour l'instant, d'utilisation d'une véritable méthode de développement de système d'information telle que Merise. Il n'y a pas de conception de jeux d'essai pour le test des nouvelles applications.

8.8 Bilan

Une analyse détaillée des moyens de la sécurité permettrait de constater que les mesures prises sont globalement en deça du souhaitable. Si la sécurité de l'exploitation est bien assurée en particulier par le plan de sauvetage et le stockage décentralisé d'une génération de copies, d'autres aspects tels que ceux concernant la protection physique sont très mal appréhendés.

9. Conclusion

La mise en œuvre d'une méthode de sécurité telle que la méthode MARION présuppose une sensibilisation de la direction aux problèmes de sécurité et un investissement conséquent de la part de l'entreprise.

Le résultat d'une telle démarche est incontestablement positif et permet non seulement de diminuer les risques mais également de susciter une prise de conscience à l'égard des risques informatiques et des conséquences que peuvent avoir un sinistre sur la viabilité de l'entreprise.

Bibliographie:

[1] J.-M. Lamère et J. Tourly: La sécurité des petits et moyens systèmes informatiques, Dunod informatique, 1988.

[2] J.-M. Lamère: La sécurité informatique, Approche méthodologique, Dunod informatique, 1985.

[3] J.-M. Lamère, Y. Leroux, J. Tourly: La sécurité des réseaux, Dunod informatique, 1987.

[4] P. Gratton: La protection des ressources informatiques, Les Editions d'Organisation, 1985.

Adresse de l'auteur:
Béatrice Simos-Rapin
C.I.G.R
Rue de la Gabelle 34
CH-1227 Carouge

Mitteilungen Communications

Verein Deutscher Ingenieure VDI jetzt auch wieder in der DDR

Ingenieure der DDR haben in Zusammenarbeit mit dem Verein Deutscher Ingenieure VDI, Düsseldorf, jetzt auch in der DDR eine Gliederung des VDI gegründet. Diese rechtlich selbständige Gliederung des VDI mit Sitz in Leipzig wurde am 11. April 1990 unter dem Namen «Verein Deutscher Ingenieure, Gliederung DDR» in das Vereinsregister eingetragen und ist für das gesamte Gebiet der DDR zuständig.
Dem 1856 gegründeten VDI war nach dem 2. Weltkrieg die Tätigkeit im Gebiet der heutigen DDR untersagt worden; der Vereinssitz wurde nach Wiederaufnahme der Vereinstätigkeit von Berlin nach Düsseldorf verlegt. In der Bundesrepublik verzeichnete der Verein einen steten Mitgliederzuwachs, so dass der VDI heute die grösste Ingenieurvereinigung Westeuropas bildet und zum Jahreswechsel 1989/90 die Zahl von 100 000 Mitgliedern überschreiten konnte.

Verein Deutscher Ingenieure VDI

Bund der öffentlich bestellten Vermessungsingenieure e.V. in der DDR

Einstimmig verabschiedeten ca. 120 Vermessungsingenieure aus der DDR eine Resolution an DDR-Innenminister Diestel, in der die Einrichtung des freien Berufs des öffentlich bestellten Vermessungsingenieures in der DDR gefordert wird. In der Resolution heisst es «Ein Monopol, wie es bisher bestanden hat, ist unbedingt zu vermeiden, um Strukturen der sozialen Marktwirtschaft herauszubilden».
Die Resolution wurde am 11. Mai 1990 bei einer Informationstagung verfasst, die der BDVI in Eichwalde/DDR zum Thema «Der öffentlich bestellte Vermessungsingenieur in der DDR» veranstaltet hat.
Auf der Tagung wurde ausserdem die Gründung eines BDVI/DDR beschlossen, der das Vermessungswesen und den Berufsstand der Vermessungsingenieure in der DDR fördern soll.

Bund der öffentlich bestellten Vermessungsingenieure e.V. BDVI

Informatik Informatique

Séminaire «systèmes d'information géographique»

La maison DEC (Digital Equipment Corporation) – Suisse S.A., le deuxième producteur mondial d'ordinateurs, a organisé le 20 juin 1990 à son siège principal suisse de Dübendorf un séminaire relatif aux systèmes d'information géographique SIG.
110 participants – parmi lesquels de nombreuses têtes connues rencontrées lors de manifestations semblables – ont été renseignés par des orateurs compétents sur l'évaluation et l'état de plusieurs projets avec des systèmes SIT/SIG.
En guise d'introduction, les participants ont apprécié l'impressionnant show audio-visuel en 3 dimensions du service des mensurations de la ville de Zurich.
Ernst Pargätzi, président de la commission SIT-Davos, a ensuite présenté le SIG intégré la région de Davos. Ce système d'information à référence spatiale pour la «plus grande ville des montagnes grisonnes» est exploité par une association de services publics et d'entreprises privées à but identique (communes, service électrique, PTT, bureaux d'in-