

Zeitschrift: Les intérêts de nos régions : bulletin de l'Association pour la défense des intérêts jurassiens
Herausgeber: Association pour la défense des intérêts jurassiens
Band: 66 (1995)
Heft: 4

Artikel: La protection des données et l'informatique : les aspects techniques
Autor: Girardin, Pierre-Robert
DOI: <https://doi.org/10.5169/seals-824401>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 13.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>



par
Pierre-Robert
Girardin,
Responsable
technique
du Centre de
gestion hospi-
talière,
Delémont.

La protection des données et l'informatique

Les aspects techniques

L'histoire de la fin du XX^e siècle sera probablement décrite comme une période de révolution : celle de la mise en place de la société de l'information. La législation sur la protection des données constitue un épisode révélateur de cette révolution et la décennie 85 - 95 aura été jalonnée de débats, de procès et de réflexions sur le thème de la protection des données. Il y a longtemps que les affaires de fichiers inquiétaient, mais il y a fort à parier que la nécessité de protéger les données n'aurait jamais été aussi nécessaire si ces mêmes données n'avaient été mémorisées, traitées, communiquées par des moyens informatiques.

En effet, dans un classeur, un tiroir, les données paraissent en sécurité ou du moins maîtrisables. Elles deviennent insaisissables, suspectes, dangereusement exploitables dès qu'elles se trouvent sur un support illisible à l'oeil. Il ne s'agit plus de parler simplement de protection des données, mais de sécurité des données. Si dans la fable, tout beau parleur vit au dépens de celui qui l'écoute, il semble qu'aujourd'hui, en matière d'informations, tout individu vive aux dépens de celui qui possède des données sur cet individu lui-même. Il ne s'agit pas de tomber dans la psychose, mais il faut admettre que les données sont une matière première de plusieurs branches économiques. La protection doit donc être prise très au sérieux.

Que faut-il protéger ?

Sur le plan technique, la protection des données est difficile à cerner. Toutefois, avant de chercher le cadre exact, il est important de s'arrêter sur l'utilisation des données. En fait, une donnée isolée n'a pas une signification forcément grande si

elle n'est pas mise en relation avec d'autres données. Une liste de températures ne sert à rien si l'on n'a aucune donnée concernant le lieu, la date et l'heure. Essayez d'imaginer tout ce que vous pourriez déduire à partir des données sur l'adresse, l'âge, le sexe, le revenu, l'endettement, les «hobbies», les films loués dans un club vidéo par une personne déterminée.

Ces données associées deviennent alors des informations. Protéger les données revient donc, sur le plan technique, à protéger aussi les informations. Cela signifie qu'il faut assurer la protection et la sécurité du système d'informations.

Qu'est-ce qu'un système d'information ?

Le cadre semble planté. Pour connaître tous les aspects de cette protection, il s'agit de définir ce qu'est un système d'information.

Un système d'informations est constitué de l'ensemble des moyens techniques, humains et organisationnels qui permet-

tent à une entreprise ou une organisation de recueillir, conserver, traiter, distribuer, présenter les informations relatives à son activité, quels qu'en soient les formes et les supports.

En d'autres termes, le système d'information englobe tant de choses que l'on peut d'emblée considérer que la sécurité des données est l'affaire de tous dans une entreprise ou une organisation.

Très concrètement, organiser la sécurité revient à mener des réflexions et à définir les mesures dans quatre domaines :

- les systèmes d'exploitation ;
- les accès et privilèges des utilisateurs ;
- la maintenance des données ;
- les locaux.

Le système d'exploitation : la sécurité au moment du choix

La décision d'utiliser l'outil informatique débouche sur le choix d'un ordinateur et d'une configuration d'ordinateurs lorsque ceux-ci sont mis en réseau. Le fonctionnement de base de la machine est déter-

miné par le système d'exploitation. Ce logiciel définit la structure des fichiers et offre l'ensemble des commandes d'accès aux données. Il est donc la première pierre de la sécurité du système d'information. Les systèmes d'exploitation les plus courants peuvent être classés en trois catégories de sécurité.

Les systèmes DOS et Windows (y compris Windows 95) n'offre quasiment aucune sécurité. Ils ont été conçus pour les ordinateurs individuels. L'accès en est facile et l'extraction, la modification ou la destruction de données est un jeu d'enfant. Ces systèmes sont d'ailleurs le terrain de prédilection des virus. On en dénombre plus de 2500 à ce jour pour ces seuls systèmes.

Plus sûrs sont les systèmes d'exploitation UNIX, OS/2 et Windows NT. Essentiellement conçus pour les configurations en réseau, ils offrent une multitude de moyens pour surveiller les accès aux données. Une configuration en réseau construite autour d'un serveur de données stratégiques ne devrait pas utiliser un système d'exploitation en-dessous de cette catégorie.

Enfin, les systèmes dits propriétaires, parce que conçus pour des machines précises, offrent la meilleure sécurité. On trouve dans cette catégorie des systèmes portant le nom de MVS (IBM), VMS (DEC), GCOS (BULL), OS400 (AS400), etc.

Il est important de relever que le choix du système d'exploitation ne doit pas seulement prendre en compte le critère de la sécurité.

Les utilisateurs

Deux questions évidentes doivent se poser quant à l'accès au système et aux privilèges des utilisateurs :

- Qui a accès ?
- Quels sont les moyens de contrôle des accès ?

Cette première barrière peut être de différentes formes :

- identification (nom, code, badge, empreinte) ;
- mots de passe (validité, règles de modification) ;
- menus personnalisés, heures de disponibilité du système.

T I B O
BUREAUTIQUE - INFORMATIQUE

PORRENTROY - DELÉMONT - LA CHAUX-DE-FONDS
066 / 66 76 76

Dans le système, les données sont mémorisées et organisées en fichiers qui constituent eux-mêmes une base de données. L'accès physique étant défini, il s'agit de régler tout l'aspect des privilèges sur les fichiers. Ceux-ci sont généralement au nombre de quatre : droit de créer, modifier, supprimer ou consulter les données.

Les données : protection, maintenance et sécurité

Au coeur du système d'information se trouvent des données qui sont créées, modifiées, effacées. La protection englobe tous les aspects de la maintenance et de la sauvegarde ; en résumé, il s'agit de garantir que les données soient utilisables.

Cette garantie d'utilisation nécessite une définition et une description écrite de trois procédures essentielles :

- les sauvegardes de sécurité ;
- l'audit du système ;
- le rétablissement du système.

Les sauvegardes de sécurité

La sauvegarde des données est un sujet sans cesse répété, car encore trop souvent négligé. Il est primordial de définir et de respecter la procédure des sauvegardes régulières, de vérifier la relecture des sauvegardes et de ranger les supports dans des lieux qui garantissent la sécurité des données sauvegardées. La localisation est très importante. Les supports ne doivent pas être dans la même

salle que l'ordinateur ; ils seront mis dans une armoire verrouillable, éventuellement anti-feu. Dans certains cas, il est recommandé d'avoir une copie dans un lieu éloigné de l'installation informatique.

L'opération de sauvegarde des données ne doit jamais être reportée !

L'audit du système

Par audit au niveau de la sécurité, il faut entendre le suivi permanent de l'utilisation du système. Les accès et les mouvements de données doivent être journalisés. Le taux d'utilisation des espaces disques doit être suivi. Les extensions du système pourront ainsi être planifiées.

Le rétablissement du système

Les données de sauvegarde ne sont pas forcément utilisées. Toutefois si les circonstances l'exigent, la procédure de rétablissement doit définir l'ensemble des opérations à effectuer, par ordre de gravité, en cas de perte de données, de panne, de destruction de machine ou même de sinistre grave.

Il faut pouvoir, remettre sur pied l'installation informatique avec les données les plus récentes. Cela va de la remise des données sur le système jusqu'à l'installation du réseau d'entreprise sur une autre installation, voire dans d'autres locaux, en passant par la redéfinition des accès et privilèges des utilisateurs.

Ce scénario doit absolument être consigné et non pas se trouver dans la tête du seul responsable système ou informatique de l'entreprise ou de l'organisation. A une époque où tout est informatisé, la

perte des données de l'entreprise peut être une catastrophe irréparable. Aucune assurance ne peut reconstituer des données perdues.

Les locaux ou bâtiments

Cet aspect ne semble plus si important. En effet, l'ère des centres de calcul, de la chambre blanche, du cerveau qu'il fallait mettre dans un local ou un bâtiment climatisé, bétonné, protégé par de multiples détecteurs est en passe de disparaître. Et pourtant la sécurité physique de la machine est devenue plus difficile aujourd'hui, car il faut tout simplement éviter de se faire emporter le serveur : en effet, un serveur de données se met actuellement sous le bras. Le vol de données peut souvent se confondre avec le vol de l'ordinateur. Il faut donc bien prendre en compte la localisation de cette machine dans l'entreprise.

Les aspects techniques de la protection des données englobent des domaines qui paraissent exagérés. C'est probablement parce que dans plusieurs cas, les données ne résident pas en totalité sur le système informatique. Une perte partielle peut être reconstituée à partir du support papier. Mais il faut tout de même relever que le support double, papier et magnétique ou optique est, d'une part coûteux à



Salle à manger séparée

✱

Salles de réunion

✱

Salles pour sociétés

✱

Plats du jour et carte

**HÔTEL : 7 CHAMBRES ENTIÈREMENT REFAITES,
COMPRENANT TÉLÉPHONE - FAX - TV**

Hôtel Restaurant de la Gare
Orfeo et Marilyn Raval

Tél. 032 - 93 10 31

2740 Moutier
Fax 032 - 93 14 11

maintenir, d'autre part dangereux du point de vue de la redondance.

La société sans papier est en préparation. Elle est déjà en pleine activité dans tous les domaines qui travaillent avec des réseaux. Elle sera aussi fiable que la société avec papier si la sécurité n'est pas négligée.

Enfin, une petite réflexion finale : parallèlement aux configurations en réseau, on

vit une expansion de l'informatique portable. Cette informatique est très vulnérable sur plusieurs aspects de la protection et de la sécurité des données. Pensez-y au moment de définir ce que vous voulez mettre dans votre ordinateur portable !

Pour terminer sur le thème de la protection, il est important de signaler que les délits à l'encontre des systèmes informatiques sont maintenant mentionnés dans le code pénal suisse. Ils sont classés en quatre catégories :

- le vol de données (ou de la machine) ;
- la copie de données (espionnage) ;
- la modification, l'effacement de données (sabotage) ;
- l'introduction d'un virus informatique (infection).

On ne répètera cependant jamais assez que les données sont une matière première et qu'aucune assurance ni aucune décision de justice ne pourront reconstituer celles qui sont perdues. Alors, nous ne pouvons que recommander vivement, une fois encore, à toutes les personnes concernées de sauvegarder leurs données souvent et régulièrement ! ■

Mobilière Suisse

Société d'assurances

l'assurance d'être bien assuré

Agence générale de Delémont
WILLY LINDER
Tél. 066 22 57 57

Agence générale de Porrentruy
HUBERT SALOMON
Tél. 066 65 92 92

Agence générale de Moutier
ERIC VEYA
Tél. 032 93 57 93

Agence générale de Saint-Imier
JEAN-PAUL VORPE
Tél. 039 41 41 55