

# Le programme en dix points pour la sécurité de l'information dans les PME

La sécurité de l'information des petites et moyennes entreprises (PME) est un thème qui acquiert de plus en plus d'importance; en effet, l'automatisation et la mise en réseau des processus commerciaux sont en constante augmentation. L'association InfoSurance montre comment disposer d'une protection de base efficace en informatique, sans grands frais ni perte de temps, grâce à son programme en dix points, simple et facile à mettre en place. Ce programme permet aux PME de prendre les mesures qui s'imposent pour améliorer la sécurité de leur information et de les appliquer elles-mêmes ou en collaboration avec leur service d'assistance informatique.



Les PME peuvent appliquer le programme en dix points en toute simplicité et indépendance. Lorsque la liste a été établie, on a plus particulièrement tenu compte des besoins et des possibilités spécifiques des PME.

Photo: Keystone

Les virus et les vers peuvent paralyser des systèmes informatiques entiers; des personnes non autorisées consultent des informations importantes et secrètes concernant les affaires et les produits d'une entreprise, tandis que des données irremplaçables appartenant à l'entreprise sont irrémédiablement perdues par manque de sauvegarde: ce sont là des menaces qui coûtent du temps et de l'argent à l'entreprise; cette dernière peut même risquer son existence. Aujourd'hui, les grandes entreprises ont compris l'importance stratégique de leurs informations et inves-

tissent pour les protéger. Quant aux PME, piliers de l'économie suisse, toutes n'ont pas encore pris conscience de la nécessité d'agir dans ce domaine.

## Des normes minimales simples à mettre en place

L'association InfoSurance – une institution créée en commun par l'État et l'économie – entend apporter sa contribution à la sécurité informatique en collaboration avec des groupements et d'autres institutions et entreprises proches des PME. Un groupe de spécialistes gravitant autour d'InfoSurance a développé une base en matière de protection informatique: le programme en dix points destiné aux PME (voir encadré 1). Les règles qu'il contient, applicables dans toutes les entreprises, doivent être considérées comme des normes minimales. La direction de l'entreprise doit les vérifier à intervalles réguliers dans le cadre de son devoir de diligence.

Les PME peuvent mettre ce programme en place en toute simplicité et indépendance. Lors de sa conception, on a tout spécialement tenu compte de leurs besoins et spécificités.



**P. Carlos Rieder**

Responsable de la sécurité de l'information à la Haute école de Lucerne – Économie, propriétaire de isec ag Lucerne, président de l'association InfoSurance

Il est évident que, pour protéger son système informatique, une PME n'a pas autant de ressources financières et humaines qu'une grande banque, par exemple. Contrairement à ce que l'on pense généralement, établir des normes élémentaires de sécurité n'engendre pas forcément des frais élevés. L'organisation et surtout la ferme volonté de l'ensemble du personnel d'appliquer ces mesures sont tout aussi importantes que les dispositifs techniques.

### La sécurité informatique n'est pas une fin en soi

La sécurité informatique n'est pas une fin en soi puisqu'elle sert à protéger les investissements et à assurer le succès de l'entreprise. Toutes les PME n'ont, du reste, pas les mêmes besoins. Certaines travaillent avec des données confidentielles très sensibles (comme les fiduciaires, les juristes, les médecins), d'autres ont besoin d'une informatique omniprésente (les entreprises de production, les graphistes, les imprimeries par exemple). Il est intéressant de constater qu'un grand nombre de PME estiment ne pas représenter un objectif rentable pour les pirates informatiques. C'est une erreur; en effet, les systèmes non protégés sont du pain bénit, car ils sont manipulés pour devenir les éléments d'un énorme «essaim» de systèmes qui, ensemble, lancent des attaques à grande échelle. Dans certains cas, des responsables d'entreprise ont dû rendre des comptes pour avoir violé leur devoir de diligence.

### Les dix points du programme

#### Responsabilité

Il faut établir les responsabilités en matière de sécurité informatique. Qui est l'interlocuteur principal? Qui est chargé de la sauvegarde des données? La sécurité de l'information est l'affaire de tous. Chaque collaborateur doit apporter sa contribution, comme respecter la confidentialité face aux personnes externes. C'est la direction de l'entreprise qui assume la responsabilité ultime. Elle doit réfléchir à cette problématique pour être à la hauteur de son devoir de diligence. Il n'est ni possible ni souhaitable qu'elle délègue sa responsabilité au service informatique.

#### Sauvegarde des données

La sauvegarde complète et régulière des données est la base de la sécurité informatique. Les données importantes doivent être sauvegardées tous les jours. La sauvegarde se fait par génération (p. ex. la bande 1 le lundi,

la bande 2 le mardi, etc.). Il est judicieux de faire des copies du travail de toute la semaine et de tout le mois. Il faut absolument contrôler que les copies sont lisibles. Les supports de sauvegarde utilisés doivent être conservés en lieu sûr, de préférence à l'extérieur de l'entreprise.

#### Protection antivirus

La protection contre les virus ou les logiciels malicieux est devenue la norme, heureusement. Il faut, toutefois, que les antivirus soient régulièrement actualisés pour ne pas perdre leur effet protecteur et devenir inutiles. Il faut donc renouveler périodiquement les abonnements de mises à jour et l'antivirus doit actualiser sa liste de signatures tous les jours. Il faut aussi vérifier que l'antivirus est lancé et qu'il fonctionne.

#### Pare-feu

On sait qu'Internet a d'innombrables avantages, mais qu'il ouvre aussi la porte aux abus. Le pare-feu contrôle les connexions entre l'ordinateur et Internet et empêche les accès illégaux. Il est primordial de surveiller les échanges depuis Internet vers l'ordinateur mais aussi dans l'autre sens. Des logiciels malicieux comme les chevaux de Troie qui parviennent à s'immiscer dans le système essaient de transmettre des données de l'entreprise vers l'extérieur. Pour contrer ces tentatives d'attaque, les pare-feu doivent être mis à jour et contrôlés régulièrement.

#### Actualisation des logiciels

Le monde des logiciels est complexe. Des erreurs peuvent s'infiltrer au cours de leur fabrication et être utilisées par des cyberpirates potentiels. Les fabricants proposent ce que l'on nomme des correctifs («patches») qui permettent d'éliminer les erreurs compromettant la sécurité. Ceux-ci doivent être installés le plus rapidement possible pour supprimer les points faibles avant qu'ils ne soient exploités. Il y a quelques années, il fallait des semaines, voire des mois, avant qu'une faille soit utilisée; actuellement, il suffit de quelques jours, ce qui rend absolument nécessaire l'installation immédiate de correctifs.

#### Mots de passe

En utilisant les mots de passe de manière inadéquate, on ouvre la porte aux usurpations d'identité. Les mots de passe sont encore considérés par le personnel de l'entreprise comme un mal nécessaire. On ferme la porte d'entrée de son entreprise avec une clé, mais on rechigne à utiliser l'économiseur d'écran avec un mot de passe. Ce dernier protège l'identité numérique et doit être manié dans la plus stricte confidentialité. Il faut

Encadré 1

#### Le programme en dix points

1. Attribution des responsabilités
2. Sauvegarde des données
3. Protection contre les virus
4. Sécurité des connexions à Internet
5. Mise à jour des logiciels; correctifs
6. Mots de passe
7. Protection des appareils portables
8. Directives pour les utilisateurs
9. Protection physique de l'infrastructure informatique
10. Classement

Encadré 2

#### L'association InfoSurance

L'association InfoSurance est une institution créée en commun par l'économie et l'État; elle vise à promouvoir la sûreté de l'information et de la communication en Suisse, en mettant l'accent sur les PME et les utilisateurs privés. Elle veut créer des conditions idéales d'organisation et d'infrastructure afin de lutter efficacement contre les risques liés à la dépendance croissante envers les technologies de l'information.

Pour de plus amples informations, veuillez consulter le site [www.infosurance.ch](http://www.infosurance.ch).



Les mesures pour assurer la sécurité informatique sont indispensables, d'autant plus lorsque les dangers viennent de l'extérieur. En illustration: inondations dans la vieille ville de Lucerne en août 2005.

Photo: Rieder

aussi qu'il soit d'excellente qualité: huit caractères au minimum, des minuscules et des majuscules, des chiffres et des caractères spéciaux, pas de noms de personnes ni de localités, etc. Si le mot de passe doit être écrit, il faut le conserver en lieu sûr et pas sur un post-it collé à l'écran ou sous le clavier!

#### Appareils portables

Les appareils portables modernes, comme les téléphones ou les assistants numériques, sont des ordinateurs de petite taille qui possèdent une énorme capacité de stockage, surtout s'il s'agit d'iPods, de lecteurs MP3, de caméras numériques ou de clés mémoire. Ils peuvent copier facilement les données d'archives entières en quelques minutes. Ces failles doivent être éliminées techniquement ou par le biais de directives. Dans tous les cas, il faut que les appareils portables soient suffisamment protégés afin que des tiers non autorisés ne puissent accéder aux données stockées.

#### Directives pour les utilisateurs

L'utilisation des appareils informatiques doit être réglementée. Quelles sont les actions autorisées ou interdites? Les directives destinées aux utilisateurs définissent comment travailler sur les ordinateurs mis à leur disposition. Peut-on installer ses propres programmes? Peut-on désactiver l'antivirus pour que les applications soient plus rapides? Peut-on stocker des données sur le disque dur local? Il faut que les réponses à ces questions soient claires. Les directives ne doivent pas rester lettre morte, tout le personnel doit les appliquer.

#### Accès à l'infrastructure

L'accès à l'entreprise doit être réglementé dans les limites du possible. Les serveurs et les appareils en réseaux doivent être mis sous clé et les tiers ne doivent pas pouvoir y accéder. Il faut aussi contrôler l'accès aux bureaux ou à la production. Toutes les mesures prises pour protéger l'informatique sont inutiles si son accès bénéficie d'un manque de surveillance des bureaux.

#### Classement

Les documents doivent être classés dans l'ordinateur de manière logique. Un archivage compréhensible et fonctionnel fait gagner du temps puisqu'il évite les recherches inutiles. Il est important que le système soit uniforme au moins au niveau des services internes. Il faut toujours ranger un poste de travail qui traite des données confidentielles avant de le quitter; la place doit être nette et les données supprimées de manière sûre. Il faut détruire le papier dans le déchiqueteur de documents. Le contenu des ordinateurs utilisés doit être effacé au moyen d'un logiciel spécial destiné à la suppression des données; dans le cas contraire, les supports doivent être détruits définitivement. ■

Encadré 3

#### Brochure et manuel sur la sécurité informatique destinés aux PME

Le programme en dix points peut être téléchargé à partir du site Internet d'InfoSurance: [www.infosurance.ch](http://www.infosurance.ch). Pour commander la version imprimée de la brochure ou pour toutes questions relatives à la sécurité informatique des PME, veuillez vous adresser à: [info@infosurance.ch](mailto:info@infosurance.ch).

Pour toute autre information, nous vous recommandons le *IT-Sicherheitshandbuch für die Praxis* (seulement en allemand). Ce manuel donne des explications de base illustrées de nombreux exemples tirés de la pratique. Les listes de contrôle et les annexes facilitent l'application. Il peut être commandé sur le site: [www.sihb.ch](http://www.sihb.ch).