SÉCURITÉ INFORMATIQUE DANS LES ENTERPRISES SUISSES

Enquête sur les menaces, la gestion des risques et les formes de coopération

Zurich, août 2006

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contact:
Center for Security Studies
Seilergraben 45-49
ETH Zentrum / SEI
CH-8092 Zurich
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch

Table des matières

Table des illustrations

Préface

La criminalité sur Internet est apparue le jour où l'ordinateur a pris le relais du stylo et du papier. Son essor a été foudroyant, dans le contexte de la globalisation des réseaux d'information. Or cette menace bien réelle n'est pas perçue comme elle le devrait. Au contraire, elle continue encore parfois de donner l'image inoffensive d'un phénomène virtuel, qui relèverait de la fiction.

Le Conseil fédéral a néanmoins pris conscience de la gravité de la situation et agi à deux reprises pour faire face aux vastes besoins présents dans ce secteur. Il a créé d'abord le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI)[1], ensuite la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)[2]. Ces structures adaptées et efficaces visent à protéger dûment la société suisse des menaces susmentionnées. Il manquait néanmoins encore une analyse approfondie du niveau de protection en place et de la menace encourue par l'économie nationale. D'autres pays procèdent depuis longtemps à de telles études. Aux Etats-Unis par exemple, le CSI/FBI publie un rapport annuel intitulé Computer Crime and Security Survey[3]. La dernière édition de ce rapport révèle notamment, documents à l'appui, que plus de la moitié des entreprises américaines interrogées ont subi une attaque informatique en 2005, et même que 95 % d'entre elles ont été victimes de défiguration de site. Plus révélateur encore, les coûts par attaque informatique ont explosé entre 2004 et 2005, passant de 51 000 à près de 300 000 US dollars en moyenne.

De telles données n'ont pas pour seule fonction de sensibiliser la population. Elles permettent de surcroît aux entreprises sondées d'établir des comparaisons, de resituer les incidents dans leur contexte, de mieux juger de l'efficacité des mesures déjà adoptées et en dernier lieu d'identifier leurs propres besoins d'agir. La réalisation de l'étude suisse a été confiée au Centre de recherche sur la politique de sécurité de l'EPF de Zurich[4].

S'ils confirment les tendances déjà connues, les résultats obtenus ont également livré des faits insoupçonnés auparavant. Les experts apprécieront sans aucun doute le rapport qui suit. Et comme il est conçu dans un langage accessible, il intéressera quiconque s'occupe de sécurité de l'information – un paramètre auquel nul ne pourra plus se soustraire à long terme.

Mauro Vignati
Analyste auprès de MELANI, Responsable du projet

1 www.scoci.ch.
2 www.melani.admin.ch.
3 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005).
4 www.css.ethz.ch.

Principaux résultats en bref

Une forte majorité des entreprises interrogées (72 %) ont signalé pour l'année 2005 au moins un incident touchant à la sécurité de l'information.
Les virus, les vers, les chevaux de Troie et les espiogiciels sont particulièrement répandus. De même, les cas de vol d'ordinateurs portables ou de matériel informatique sont monnaie courante. En revanche, les attaques par déni de service, le piratage, le vol de données et la défiguration de sites sont plus rares.

Les entreprises de plus de 250 salariés et celles qui achètent ou vendent via Internet sont davantage exposées aux incidents.
Les grandes entreprises, de même que les sociétés pratiquant le e-commerce, sont des proies idéales pour des attaques ciblées.

Presque toutes les entreprises recourent à des mesures techniques ou organisationnelles de protection.
Les mesures techniques les plus courantes sont les logiciels antivirus et les pare-feu, utilisés par la quasi-totalité des entreprises. Sur le plan organisationnel, la mesure la plus répandue est la gestion des sauvegardes. Quant aux mesures techniques et organisationnelles plus complexes (comme les organisations de crise), elles s'utilisent avant tout dans les grandes entreprises et dans les sociétés de la branche informatique.

Les entreprises n'ont que peu de moyens financiers et de personnel à disposition dans le domaine de la sécurité de l'information.
En outre, seule une minorité des entreprises interrogées (32 %) confient à un informaticien qualifié les questions liées à la sécurité de l'information.

Beaucoup d'entreprises externalisent leurs risques liés à la sécurité de l'information.
L'externalisation est particulièrement courante dans les moyennes entreprises. Il est fréquent aussi d'assurer les dommages potentiels liés aux problèmes de sécurité de l'information.

Bien des entreprises seraient favorables au renforcement de la coopération entre elles.
Une majorité d'entre elles juge nécessaire de créer de nouvelles organisations pour la coopération. Le cas échéant, il s'agira de prendre en compte la grande diversité des besoins des entreprises.

1 Introduction

Les technologies de l'information et de la communication (TIC) imprègnent le quotidien de la plupart des entreprises ou autorités suisses. Elles permettent d'effectuer un travail en réseau et simplifient la communication. Or le recours à ces nouvelles technologies est à l'origine de problèmes inconnus auparavant. Alors que l'on doutait encore dans les années 1980 de l'existence de virus informatiques, ils sont aujourd'hui répandus dans le monde entier et créent toutes sortes de menaces pour la sécurité informatique.

La dépendance grandissante des TIC dans toutes sortes de secteurs et la négligence parfois constatée dans l'usage qui en est fait augmentent le risque de pannes, lesquelles affectent à leur tour le fonctionnement des processus économiques. Un dysfonctionnement des TIC coûterait très cher à l'économie suisse. Une étude du Computer Engineering and Networks Laboratory (TIK) de l'EPF de Zurich a ainsi chiffré à 5,83 milliards de francs les dégâts que causerait une panne Internet d'une semaine. Cette étude montre à quel point une société moderne comme la nôtre est dépendante de l'informatique et d'Internet. Concrètement, 48 % des 3,6 millions d'emplois que compte la Suisse sont tributaires des TIC.[5]

Cette situation justifie que les entreprises prennent une série de mesures – selon leurs besoins de sécurité et les moyens à disposition. Les possibilités dans ce domaine vont de l'adoption de mesures techniques ou organisationnelles de protection à la sensibilisation générale du personnel.

La présente étude vise à donner un aperçu des menaces guettant l'économie suisse dans le domaine de la sûreté de l'information et à indiquer comment des entreprises ou des autorités peuvent y faire face. En outre, elle vise à savoir si une coopération entre entreprises serait envisageable ponctuellement et comment l'Etat pourrait soutenir les sociétés afin de protéger leurs TIC.

1.1 Méthode de l'étude

L'enquête a été réalisée par écrit auprès d'entreprises ou d'autorités de toutes tailles, provenant de l'ensemble de la Suisse et de toutes les branches des secteurs secondaire et tertiaire (industrie et services), par souci d'obtenir la meilleure vue d'ensemble possible. Concrètement, 4916 entreprises ou autorités ont été contactées par courriel ou par lettre.[6] Mais au lieu de recevoir un document préimprimé, elles étaient invitées à télécharger le questionnaire d'Internet à l'aide d'un mot de passe, de façon à réduire au maximum le fardeau administratif. Le questionnaire comportait 36 questions et les participants à l'étude avaient quatre semaines pour le remplir (du 15 mars au 13 avril 2006).[7] Il a été complété à 562 reprises pendant cette période. Le taux de retour est ainsi de 11,45 %, chiffre correspondant à la moyenne des enquêtes similaires.[8]

1.2 Etat de la recherche et études comparatives

La plupart des études antérieures consacrées à la sécurité des TIC n'abordent que les aspects techniques ou sont conçues sous forme de recommandations pratiques aux responsables des

5 Dübendorfer, Thomas, Arno Wagner et Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (étude du Computer Engineering and Networks Laboratory de l'EPF de Zurich, 2004), p. 4.
6 Sur le choix et la composition de l'échantillon, voir annexe 1.
7 Le questionnaire et des précisions sur la méthode d'enquête figurent à l'annexe 5.
8 Une évaluation détaillée des retours figure à l'annexe 2.

entreprises. Ainsi il n'existe à ce jour aucun état des lieux de la sécurité de l'information des entreprises suisses. La présente étude se fonde néanmoins sur l'enquête publiée en 2002 par la Task Force PME sous le titre «Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz»[9], dans la mesure où il importait de connaître l'importance de l'informatique dans les diverses entreprises pour analyser la sécurité de l'information.

Comme d'autres pays ont déjà mené des analyses complètes de la sécurité de l'information dans les entreprises, des comparaisons s'imposaient avec les études internationales. Les principales sources d'information sont la «FBI Computer Crime Survey 2005»[10], l'étude «Hi-Tech Crime: The Impact on UK Business 2005» de l'agence britannique National Hi-Tech Crime Unit[11], ainsi que le rapport de l'Office fédéral de la sécurité dans la technologie de l'information (BSI)[12] «Die Lage der IT-Sicherheit in Deutschland 2005».

1.3 Terminologie

Les définitions ci-dessous concernent les notions le plus fréquemment employées dans la présente étude.

Sécurité de l'information
La sécurité de l'information vise à empêcher toute modification ou acquisition non autorisée d'informations ou de données. Outre des mesures techniques (portant sur le système), le processus servant à garantir qu'une sécurité de l'information maximale soit réalisée passe par des mesures organisationnelles ou d'exploitation.

Objectifs de protection dans la sécurité de l'information
Authenticité: L'authenticité d'un objet (p. ex. données, systèmes, serveurs, etc.) ou d'un sujet (User) signifie que l'identité indiquée est véritable. Elle doit être contrôlable à l'aide de propriétés spécifiques.
Intégrité des données: L'intégrité des données est garantie lorsque ni les sujets ni les objets n'ont la possibilité de modifier sans autorisation les données à protéger.
Confidentialité: Un système garantit la confidentialité s'il empêche de se procurer des informations sans autorisation préalable, y compris pendant le transport des données.
Disponibilité: Un système est réputé disponible si les sujets dûment authentifiés et autorisés ne subissent aucune restriction qui n'aurait pas été autorisée dans l'exercice de leurs droits.

Vulnérabilité
Par vulnérabilité, il faut entendre une faille du système susceptible de mettre en péril les objectifs de protection définis plus haut. Elle peut exister face à des dangers physiques (incendie, dégât d'eau, tremblement de terre, foudre, panne de courant), à une utilisation inadaptée ou p. ex. des maliciels.

9 Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (étude réalisée sur mandat du Secrétariat d'Etat à l'économie, Berne, 2002; résumé en français).

10 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), 2005 Computer Crime and Security Survey (2005). www.gocsi.com.

11 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005). www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

12 Bundesamt für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2005* (juillet 2005). www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf.

Menace
Le système doit être qualifié de menacé s'il présente un ou plusieurs aspects vulnérables, susceptibles d'affecter les objectifs de protection définis ci-dessus.

Risque
Le risque signale la probabilité (fréquence relative) d'un événement dommageable, ainsi que les coûts qui s'ensuivent. Le risque dépend également du montant des valeurs à protéger.

Attaque / Incident
Une attaque désigne un accès ou une tentative d'accès non autorisés à un système. On distingue entre les attaques passives (obtention sans autorisation d'informations, perte de confidentialité) et les attaques actives (modification non autorisée des données, perte de l'intégrité, perte de disponibilité).[13]
La présente étude emploie toutefois le terme plus général d'incidents, pour bien montrer que les fausses manipulations involontaires risquent elles aussi de causer des problèmes sur le plan de la sécurité de l'information.

13 Les définitions sont reprises, sous une forme simplifiée et résumée, de: Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (3e éd. remaniée et complétée, Munich et Oldenbourg 2004), p. 4 à 17.

2 Fréquence des incidents

Cette première partie de l'analyse a pour objet la fréquence des incidents, la menace que les collaborateurs constituent pour la sécurité de l'information ainsi que le risque de survenance d'un incident en fonction du genre d'entreprise et de la forme de menace. Un premier sous-chapitre définit et explique les menaces relevant de la sécurité de l'information. Ces considérations sont très brèves, étant donné la facilité de se procurer des compléments d'information via Internet et dans les publications.[14]

2.1 Menaces pour la sécurité de l'information

Les entreprises ont été questionnées sur les principales menaces connues sur le plan de la sécurité de l'information. De telles menaces affectent en principe la confidentialité, la disponibilité et l'intégrité des données. En revanche l'enquête ne porte pas sur les pourriels (spams, junk mails), et donc sur la publicité électronique non désirée. En effet, ces courriels ont beau être importuns, ils ne menacent généralement pas directement la sécurité de l'information.

2.1.1 Description des menaces examinées

Virus, espiogiciels, vers et chevaux de Troie (malware)
Un *virus* consiste en instructions programmées pour obliger un ordinateur à effectuer certaines actions. Pour continuer à se propager, il s'installe dans un «programme hôte», qui peut être une application (p. ex. logiciels téléchargés) ou un document (p. ex. fichier Word, fichier Excel). L'exécution de l'application ou l'ouverture du document ont pour effet d'activer le virus. L'ordinateur est ainsi amené à réaliser des actions dommageables. Les virus proviennent souvent d'annexes de courriels ou de fichiers infectés téléchargés d'Internet. Une fois activés, ils peuvent se réexpédier par courriel aux contacts du carnet d'adresses. Les autres moyens de propagation sont les supports de données externes (p. ex. CD-ROM, clé mémoire USB, etc.).

Un *espiogiciel* (*spyware*) peut collecter des informations à l'insu de l'utilisateur puis les transférer à une adresse prédéfinie. Les informations recueillies varient d'un l'espiogiciel à l'autre et vont des habitudes de navigation aux réglages du système, en passant par les mots de passe ou les documents confidentiels.

A l'instar des virus, les *vers* consistent en instructions programmées pour amener l'ordinateur à effectuer certaines actions. Mais contrairement aux virus, ils n'ont besoin d'aucun programme hôte pour se propager. Au contraire, les vers tirent parti des failles de sécurité ou des erreurs de configuration d'un système d'exploitation ou d'une application. Un ver peut prendre pour cibles des ordinateurs qui présentent des lacunes de sécurité ou des erreurs de configuration, dès lors qu'ils sont reliés à d'autres ordinateurs (p. ex. via Internet ou le réseau local, etc.).

Les *chevaux de Troie* sont des programmes qui exécutent en cachette des actions dommageables, en se faisant passer auprès de l'utilisateur pour des applications ou fichiers utiles. Les chevaux de Troie sont bien souvent des programmes téléchargés d'Internet. Il peut également s'agir de morceaux de musique ou de films. Ils tirent parti de failles de sécurité dans les programmes joués

14 Informations publiées sous: www.melani.admin.ch/gefahren-schutz/gefahren/index.html?lang=fr. On trouve dans la littérature beaucoup d'ouvrages de synthèse sur la sécurité de l'information. Des informations complètes figurent dans: Bidgoli, Hossein et al. (éd.), *Handbook of Information Security Volume 3* (Hoboken, 2006).

(p. ex. Media Player) pour s'installer discrètement sur le système. Les chevaux de Troie se propagent fréquemment aussi par les annexes de courriels. Ils servent généralement à espionner des données confidentielles, à prendre le contrôle complet de l'ordinateur ou à envoyer des pourriels sur l'ordinateur infecté.

Attaques par déni de service (Denial of Service, DoS)
Les attaques par déni de service visent à rendre un service inaccessible aux utilisateurs ou du moins à en limiter sérieusement la disponibilité. Une variante populaire des attaques DoS consiste à assaillir de demandes un ordinateur/service. Sous l'effet de la surcharge, l'ordinateur/le service a besoin d'énormément de temps pour répondre ou tombe en panne.

Ces attaques proviennent souvent de nombreux ordinateurs manipulés au préalable à l'aide de programmes malveillants. On parle alors d'attaques par déni de service distribué (Distributed Denial of Service, DDoS). Elles visent principalement les entreprises qui souhaitent effectuer des affaires via Internet et vont souvent de pair avec des actes de chantage.
Comme beaucoup d'ordinateurs sont infectés par des maliciels (malware) sans que personne ne s'en doute et donc que des pirates pourraient profiter de la situation, les menaces dues aux attaques DDoS augmentent. En effet, si plusieurs ordinateurs sont manipulés pour constituer un réseau (réseau de zombies), les attaques DDoS s'en trouvent facilitées. Les experts mettent donc en garde contre le risque d'augmentation de telles attaques.

Intrusion dans le système (hacking) et vol de données
Le hacking, ou piratage informatique, n'est pas une notion précisément définie, mais porte sur toutes sortes de manipulations non autorisées effectuées sur des ordinateurs étrangers. Le hacking décrit l'intrusion non autorisée dans le système informatique d'une entreprise. Il consiste souvent à utiliser des programmes d'espionnage ciblés (espiogiciels, chevaux de Troie). Les pirates peuvent lire, modifier ou effacer les données du système dans lequel ils ont pénétré. Les plus graves dommages sont dus à des pirates animés de mobiles criminels, qui s'emparent des données d'une entreprise. Leurs attaques prennent souvent pour cible les données confidentielles de clients ou les idées nouvellement développées, dont dépend la survie économique des entreprises. Un vol de données peut donc être lourd de conséquences pour une entreprise. Ce type d'attaques est généralement très difficile à déceler.

Défiguration de site (defacement)
La défiguration d'un ou plusieurs sites (mass defacement) consiste à tirer parti des lacunes de sécurité de serveurs Web. Les pirates modifient le contenu et le graphisme des sites. Leurs attaques ont parfois des mobiles politiques et sont l'oeuvre de «hacktivistes» cherchant à donner de l'audience à leurs protestations. Bien souvent ce sont des adolescents, les «script kiddies», qui défigurent des sites par jeu. Selon l'importance que revêt le site pour l'activité économique de l'entreprise victime, les conséquences d'une attaque vont des dégâts d'image à de lourdes pertes d'ordre financier.

Abus des réseaux sans fil
Les réseaux locaux sans fil (Wireless Local Area Network, WLAN) procurent un accès sans fil et aisé à Internet. Or bien souvent ils sont trop peu protégés, et donc des pirates sont susceptibles de s'immiscer dans la connexion à diverses fins. Ces accès mal protégés sont problématiques parce que les abus sont généralement découverts tardivement, voire demeurent inaperçus.

Vol d'ordinateurs portables et d'autre matériel informatique
Malgré toutes les nouvelles formes de menaces, il ne faut pas oublier que le matériel informatique reste exposé au vol. Outre la perte liée à sa valeur intrinsèque, d'importants dégâts supplémentaires sont possibles, par exemple si un ordinateur dérobé contenait des données sensibles.

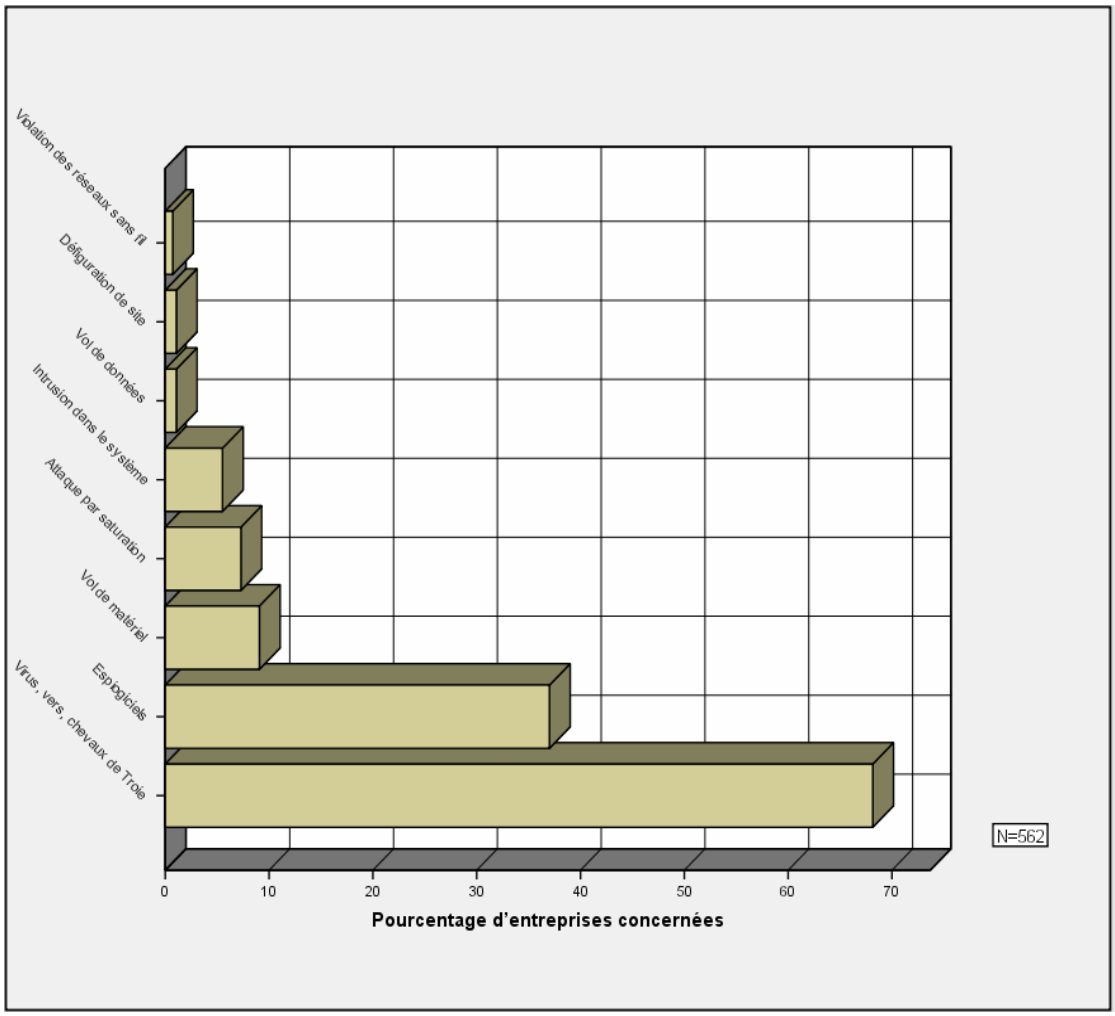
2.1.2 Fréquence des incidents

L'enquête visait à déterminer si les entreprises avaient subi en 2005 l'une des menaces susmentionnées. Les dépouillements effectués montrent que les incidents sont fréquents dans le domaine de la sécurité de l'information. Ainsi, pas moins de 72 % des sociétés ayant pris part à l'enquête signalent qu'au moins une des menaces susmentionnées a causé un incident dans leur infrastructure de l'information. Il faut néanmoins prendre en compte que la participation à l'enquête n'est guère représentative de la réalité. A titre d'exemple, 15 % des participants sont des entreprises de plus de 250 salariés, alors que seules 0,4 % des sociétés possèdent cette taille. En outre, certaines branches sont surreprésentées par rapport à la réalité.[15] D'où l'impossibilité d'inférer directement de l'enquête des conclusions valables pour l'ensemble des entreprises du secteur secondaire et du secteur tertiaire. L'outil statistique de la pondération permet néanmoins de juger de la fréquence réelle des incidents. Concrètement, une simulation évalue de façon différenciée les données des entreprises.[16] Le recours à cette procédure permet d'estimer à 63 % la part des entreprises suisses ayant déploré durant l'année 2005 au moins l'un des incidents faisant l'objet du présent rapport.

Comme les diverses menaces ont des conséquences plus ou moins lourdes, il est important d'en connaître la fréquence. La fig. 1 montre quel pourcentage des entreprises ou autorités questionnées a subi chaque type d'incidents.

15 L'annexe 2 montre les retours en fonction de la taille des entreprises et de la branche d'activité.
16 Toutes les données ont été multipliées par un facteur de pondération. Des précisions sur la procédure utilisée figurent à l'annexe 3.

Fig. 1 Fréquence des incidents



Les maliciels (virus, vers, chevaux de Troie et espiogiciels) sont de loin les plus répandus. Le vol de matériel informatique figure en troisième position. Quant aux attaques qui sont techniquement plus sophistiquées et présentent des conséquences graves, il est bien plus rare qu'elles soient découvertes.

2.1.3 Menace due au personnel

Le fait de connaître la fréquence des incidents aide à évaluer les risques courus par les entreprises. Il importe non moins de connaître l'origine des incidents. Il est notamment intéressant de savoir quel genre de dommages les collaborateurs sont susceptibles de causer.

Le personnel est susceptible de menacer la sécurité de l'information à divers titres. D'abord il risque de faciliter l'apparition de maliciels ou d'attaques ciblées par un comportement inadéquat, ensuite il peut être à l'origine d'attaques – par exemple par appât du gain, ou bien par vengeance envers des supérieurs. Beaucoup d'experts estiment que les collaborateurs sont directement res-

ponsables d'une part importante des incidents.[17] L'étude britannique «Hi-Tech Crime: The Impact on UK Business 2005» a montré qu'une fraction importante des incidents sont commis de l'intérieur. Selon cette étude, 37 % des incidents enregistrés dans des entreprises britanniques proviendraient de manipulations volontaires d'employés déloyaux ou insatisfaits.[18] Le pourcentage correspondant dans la présente étude est de 10 % des entreprises questionnées, soit un chiffre bien inférieur aux attentes. Il n'est toutefois pas possible de faire de comparaison directe avec l'étude britannique, qui concerne en partie d'autres menaces et se limite aux entreprises de plus de 100 collaborateurs.

Force est néanmoins de constater que les incidents directement imputables à un collaborateur sont plutôt rares en Suisse. Les cas d'employés causant délibérément des dommages restent en effet l'exception. Les fautes involontaires s'avèrent donc bien plus menaçantes pour la sécurité de l'information.

2.1.4 Fréquence des incidents en comparaison internationale

Quelle est la fréquence des incidents constatés par rapport aux études étrangères? Quelque 87 % des participants à la «Computer Crime Survey» de 2005 signalent avoir subi un incident. Cette enquête de grande envergure due au FBI ne recense toutefois que les entreprises de plus de cinq postes à plein temps. Autrement dit, il faut exclure les entreprises de moins de cinq personnes lors des comparaisons. De toutes les entreprises et autorités de Suisse qui comptent plus de cinq employés, 79 % signalent avoir subi un incident. Ce chiffre est un peu inférieur à celui du FBI, qui se fonde sur une définition plus large des incidents. A titre d'exemple, son étude recense parmi les incidents la découverte de matériel pornographique.

De même, l'étude britannique déjà citée «Hi-Tech Crime: The Impact on UK Business 2005» montre que la Suisse connaît les mêmes problèmes que les autres pays dans le domaine de la sécurité de l'information. Cette enquête menée parmi les entreprises de plus de 100 employés révèle que 89 % des sociétés ont subi un incident en 2004. Dans la même catégorie, 85 % des entreprises suisses sont concernées.

Quant au genre des incidents, les résultats correspondent à peu près à ceux des études internationales. De même, l'étude du FBI révèle que les virus et les espiogiciels sont de loin le problème le plus fréquent, que les vols de matériel sont fréquents et les attaques ciblées plutôt rares.

En conclusion, les entreprises suisses ne subissent ni plus ni moins d'incidents que celles d'autres pays. A l'ère des réseaux mondialisés, les menaces concernant la sécurité de l'information sont en effet partout équivalentes.

2.2 Risque d'incident par catégorie d'entreprise

Alors que la nationalité des entreprises n'a pas d'impact décisif sur le risque d'incident, il est permis de supposer que leur taille et leur champ d'activité affectent la probabilité d'être victimes

17 Un rapport de Gartner considère même que 70 % des abus informatiques sont dus au personnel. Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Synthèse des résultats sous: www.csoonline.com/analyst/report3317.html. En Allemagne, l'Office fédéral de la sécurité dans la technologie de l'information juge lui aussi très élevée la proportion de tels délits: Bundesamt für IT-Sicherheit, *Die Lage der IT-Sicherheit in Deutschland 2005* (juillet 2005), p. 29.

18 The National Hi-Tech Crime Unit (nhctu), *Hi-Tech Crime, The Impact on UK Business 2005* (2005), p. 20.

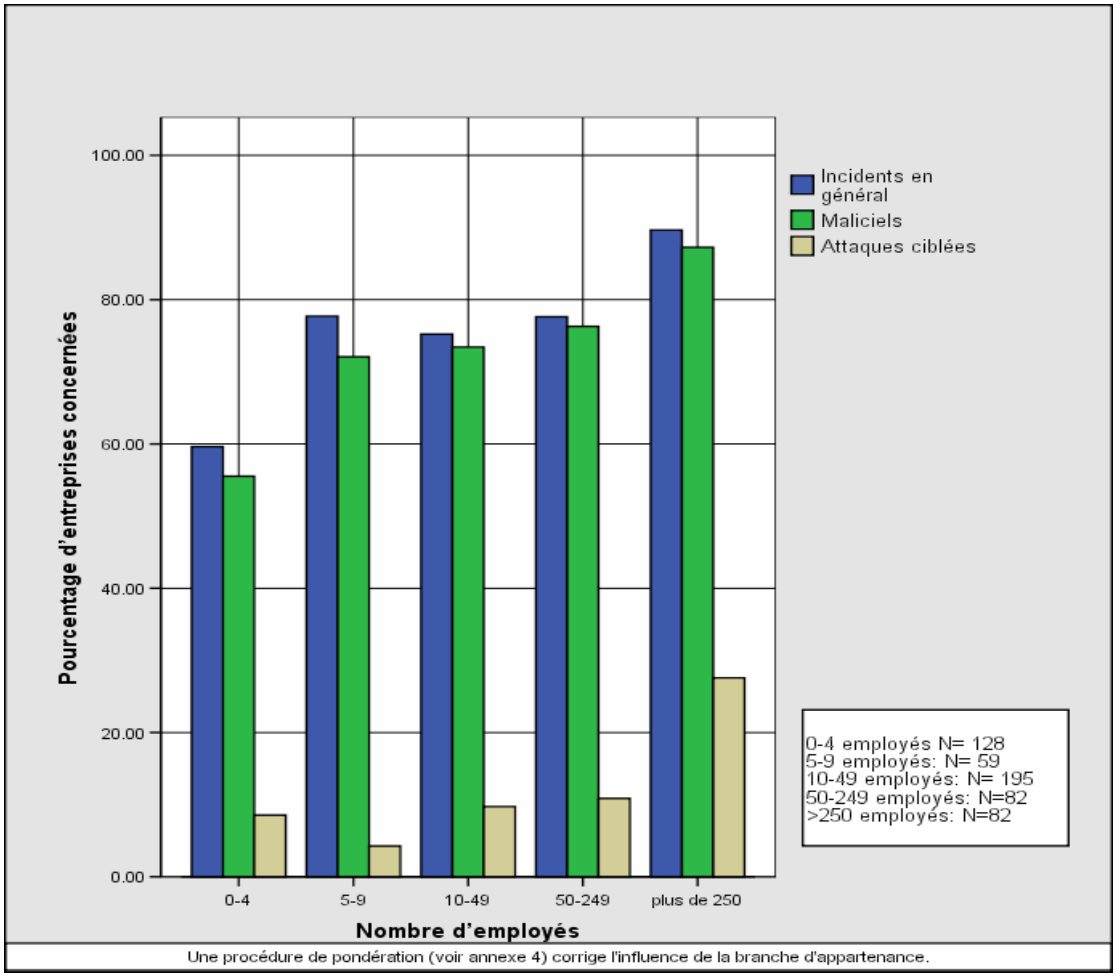
de maliciels et d'attaques ciblées. Cette section examine les catégories d'entreprises les plus exposées à de tels incidents.

2.2.1 Risque selon la taille de l'entreprise

L'étude de la Taskforce PME concernant la place de l'informatique et d'Internet dans les entreprises a montré l'existence d'un lien entre la taille de l'entreprise et l'usage fait de l'informatique. Plus une société est grande, plus les TIC y jouent un rôle important.[19] Or le recours accru à ces moyens accroît également le risque d'incidents. A titre d'exemple, plus les collaborateurs envoient et reçoivent de courriels, plus le risque est grand que des virus pénètrent dans le réseau d'entreprise. En outre, les grandes entreprises sont plus attrayantes pour les attaques ciblées. En effet, une société doit réaliser un certain chiffre d'affaires ou disposer d'un patrimoine suffisant pour justifier les coûts liés à une attaque ou un détournement. A ce propos, les grandes entreprises offrent naturellement de meilleures perspectives aux pirates que les petites.

La fig. 2 montre que la probabilité que survienne un accident augmente avec la taille de l'entreprise.

Fig. 2 Risque d'incident en fonction de la taille de l'entreprise



19 Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen* (Berne 2002), p. 19.

Les incidents sont sensiblement plus rares parmi les entreprises de moins de cinq collaborateurs. Les PME (5 à 9, 10 à 49 et 50 à 249 collaborateurs) forment un groupe homogène. Elles rencontrent certes nettement plus de problèmes dus aux maliciels, mais sans subir beaucoup plus d'attaques ciblées que les plus petites entreprises. En effet, les attaques ciblées concernent en premier lieu les entreprises comptant plus de 250 collaborateurs. 28 % des sociétés de cette catégorie ont signalé une telle attaque. Les maliciels visent également plus souvent les grandes entreprises que les PME.

Ainsi les résultats sont conformes aux attentes. La différence entre les micro-entreprises et les grandes entreprises est flagrante. Il est surprenant toutefois de constater l'absence de différence notoire entre les petites entreprises de 5 à 9 collaborateurs et les moyennes entreprises qui en comptent jusqu'à 249.

2.2.2 Risque par secteur d'activité

La classification par branche[20] est habituellement utilisée pour différencier les entreprises en fonction de l'activité exercée. L'hypothèse étant que les entreprises d'une même branche développent leurs activités de manière similaire. La présente étude passe donc en revue les risques courus dans chaque branche.

Outre la taille d'une entreprise, sa branche d'appartenance a une influence sur le rôle joué par les technologies informatiques et Internet.[21] Aussi est-il permis de supposer que le risque d'attaques ciblées n'est pas le même dans toutes les branches, a fortiori si certaines réalisent d'importants chiffres d'affaires ou disposent de capitaux exposés aux attaques basées sur les TIC. D'où l'hypothèse que les entreprises p. ex. du secteur financier ou de la branche informatique, qui recourent beaucoup à l'informatique et génèrent d'importants chiffres d'affaires, enregistrent plus d'incidents que celles du secteur de la construction ou de l'hôtellerie-restauration.

Or le dépouillement de l'enquête ne confirme pas cette hypothèse. Car même si les entreprises de la branche informatique sont particulièrement exposées aux incidents, les entreprises de services financiers n'en subissent pas davantage que celles de l'hôtellerie-restauration.[22] Cet écart par rapport aux attentes pourrait tenir au fait que les branches ne se protègent pas toutes aussi soigneusement.[23]

La différenciation par branche n'est d'ailleurs peut-être pas adéquate pour déterminer, sur la base du genre d'activité exercée, le risque d'incident encouru. En effet, les technologies informatiques ou Internet peuvent jouer un rôle très différent au sein d'une même branche. Pour être pertinent par rapport au risque, le critère de l'activité exercée devra donc se référer davantage à l'utilisation faite des technologies informatiques et Internet – comme les achats et les ventes par Internet.

20 On distingue ici douze branches. Des précisions sur la répartition par branche figurent à l'annexe 1.

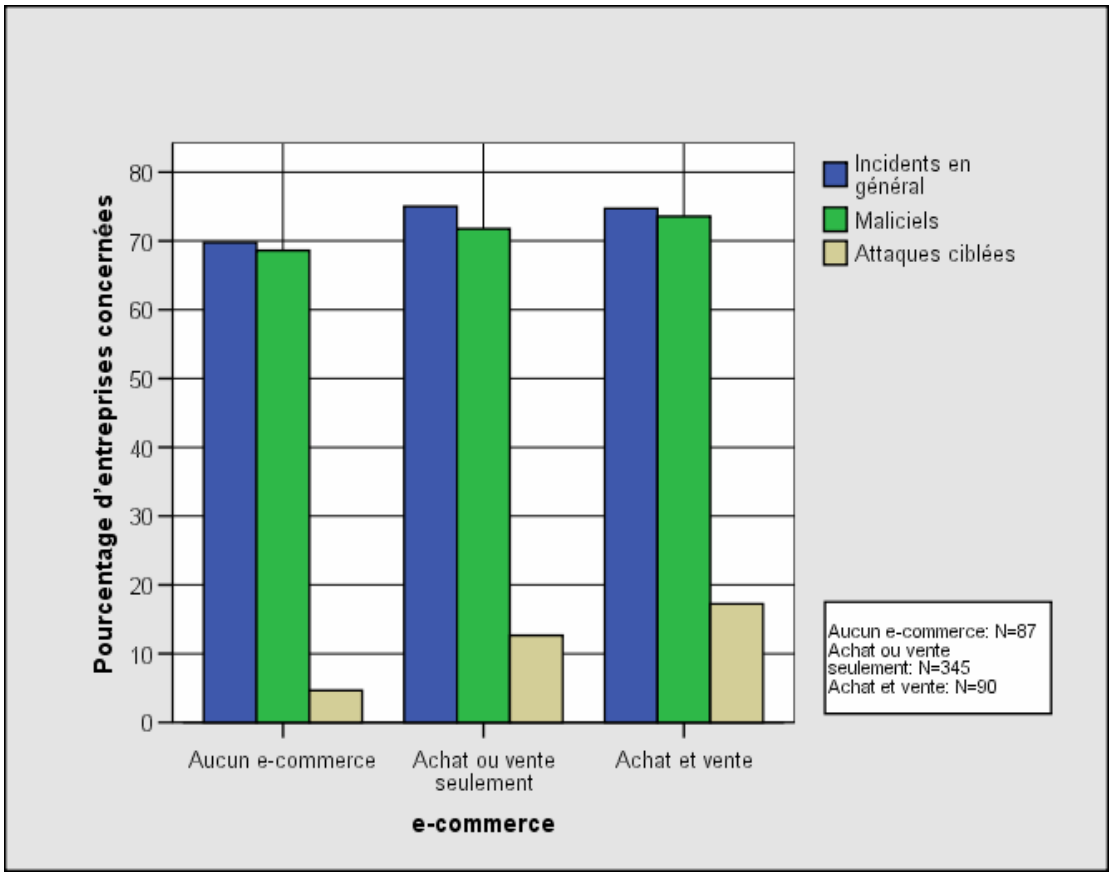
21 Les résultats de l'enquête correspondent à ceux de l'étude de la Task Force PME. Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Berne, 2002), p. 20.

22 Les résultats pondérés selon l'importance de la branche montrent que 71 % des entreprises du secteur financier et 73 % de celles de l'hôtellerie-restauration ont constaté un incident. Les pourcentages les plus élevés concernent les sociétés de services aux entreprises (86 %), tandis que les entreprises de la branche commerciale sont les moins touchées (61 %).

23 Le chapitre 3 est consacré à la gestion des risques.

Le commerce en ligne est devenu très important pour les entreprises suisses. 77 % des sociétés interrogées signalent acheter des produits ou des services via Internet.[24] Elles sont toutefois bien moins nombreuses (19 %) à vendre des produits ou des services sur leur site Internet.[25] D'où l'hypothèse que les entreprises recourant au e-commerce risquent davantage de constater des incidents, et en particulier qu'elles font plus souvent l'objet d'attaques ciblées.

Fig. 3 Risque d'incident en fonction de l'activité déployée dans le e-commerce



La fig. 3 confirme clairement cette hypothèse. Ainsi les entreprises qui pratiquent le e-commerce sont nettement plus sujettes aux attaques ciblées. 12 % des entreprises qui vendent ou achètent par Internet, et même 17 % de celles qui font les deux à la fois ont signalé de telles attaques, alors même que les attaques non ciblées de maliciels n'augmentaient que légèrement dans leur cas. Quant aux sociétés qui ne font pas de e-commerce, elles ont beau enregistrer presque autant d'incidents, seules 5 % ont fait l'objet d'attaques ciblées.

La supposition voulant que les entreprises pratiquant le commerce électronique subissent davantage d'attaques ciblées se vérifie donc. Pour estimer le risque lié aux maliciels en général, il n'est guère important en revanche qu'une entreprise effectue des transactions par Internet. En ef-

24 Même après pondération statistique (voir annexe 3), elles sont encore 73 % dans ce cas. Ce chiffre très élevé correspond aux études antérieures consacrées au e-commerce. Il ressort ainsi de l'étude Netzreport 02 (2001) que 60 % des entreprises font des achats par Internet. En revanche, l'étude de la Task Force PME avançait un chiffre de 29 % seulement (Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Berne, 2002), p. 32).

25 Ce chiffre tombe à 14 % si l'on se réfère à l'ensemble des entreprises suisses, par la procédure de pondération (voir annexe 3).

fet, comme les virus, vers, chevaux de Troie ou espiogiciels non programmés pour une utilisation spécifique et individualisée sont bien plus répandus et qu'ils attaquent au hasard les systèmes vulnérables sans viser en premier lieu les activités commerciales des entreprises, les maliciels sont tout aussi probables parmi les entreprises ne concluant pas leurs transactions via Internet.

2.2.3 Bilan et autres moyens de contrôle des risques

Il s'avère que certaines entreprises courent un risque d'incident accru dans le domaine de la sécurité de l'information. Leur taille et l'usage commercial qu'elles font d'Internet sont déterminants.

Outre la taille des entreprises et l'activité qu'elles déploient, d'autres facteurs sont également susceptibles d'influencer le risque d'incident, comme le genre de liaison Internet, le stade d'innovation technique atteint ou la notoriété de l'entreprise. D'où la nécessité de procéder à d'autres analyses complètes pour être en mesure de prédire les menaces pesant sur la sécurité de l'information dans telle ou telle entreprise.

On peut toutefois se demander si de tels travaux seraient réalistes. En effet, lors des analyses des risques par catégorie d'entreprises, il ne faut pas oublier que les sociétés n'ont indiqué que les incidents qu'elles avaient découverts, et que bien souvent les attaques ciblées ne sont remarquées que tardivement.

En outre, il faut se rappeler que les entreprises réagissent différemment aux menaces affectant la sécurité de l'information. Ainsi les mesures techniques et organisationnelles de protection réduisent la probabilité d'un incident en repoussant de bonne heure les menaces ou en réduisant les vulnérabilités existantes, si bien que malgré un contexte tout aussi menaçant le risque diminue. En même temps, de meilleures mesures de protection au sein des entreprises font que les incidents sont découverts plus rapidement. Aussi le chapitre suivant examine-t-il de près la gestion des risques en place dans les entreprises.

3 Gestion des risques

Le champ des mesures potentielles contre les menaces affectant la sécurité de l'information est à la mesure de la diversité de ces menaces. La gestion des risques repose sur des mesures techniques, mais inclut aussi des questions stratégiques et organisationnelles. Ce chapitre passe séparément en revue divers volets de la gestion des risques, dans le souci de ne pas perdre la vue d'ensemble.

Les mesures techniques et organisationnelles et leur implantation dans les entreprises seront analysées dans un premier temps. Après quoi nous examinerons les ressources financières et en personnel affectées par les sociétés à la sécurité de l'information. Comme les entreprises cherchent généralement à limiter au strict minimum les moyens alloués à la sécurité de l'information, il est intéressant d'étudier si l'on constate des différences significatives entre elles. Enfin, une dernière section analyse à quelle fréquence les entreprises suisses délèguent leurs tâches en la matière à des spécialistes externes et si elles tentent au passage de faire couvrir leurs risques par des assurances.

3.1 Mesures techniques et organisationnelles de protection

En matière de gestion des risques, il est crucial que chaque entreprise prenne les mesures les plus adéquates. Ce chapitre analyse les possibilités auxquelles les entreprises recourent le plus souvent. Par souci de clarté, une distinction est faite entre les mesures techniques et organisationnelles.

3.1.1 Définition des mesures techniques

Avant d'en venir à la fréquence d'utilisation des mesures, il importe de définir brièvement ces dernières. Là encore, des renvois sont faits aux informations disponibles sur Internet et dans la littérature.[26]

Programmes antivirus
Les programmes antivirus font partie des mesures techniques élémentaires destinées à protéger la sécurité informatique. Ils détectent les maliciels qui se sont introduits sur l'ordinateur et les bloquent ou les éliminent. Pour que l'opération réussisse, il faut connaître tous les spécimens de maliciels. Comme de nouveaux virus ou vers apparaissent constamment, il est nécessaire de tenir à jour les antivirus.

Pare-feu
Les pare-feu ont pour but de protéger les systèmes informatiques des intrusions indésirables ou des menaces dues aux maliciels. A cet effet, ils surveillent les liaisons entrantes ou sortantes, rejetant les liaisons indésirables. Les pare-feu font partie des mesures techniques de base, et les entreprises les installent généralement à l'interface entre Internet et leur propre réseau.

Cryptage (encryption)
Dès le moment où des informations sensibles sont enregistrées dans des réseaux informatiques, des personnes non autorisées sont susceptibles d'y accéder. La même menace existe lors de la communication de données confidentielles (p. ex. par courriel). Aussi des programmes de

26 www.melani.admin.ch/gefahren-schutz/gefahren/index.html?lang=fr. Ces mesures sont décrites en détail dans: Bidgoli, Hossein et al. (éd.) *Handbook of Information Security Volume 3* (Hoboken, 2006).

cryptage sont-ils utilisés. Les données sont converties en texte chiffré, selon une procédure de cryptage spécifique (algorithme) que seule une personne possédant la clé correspondante sera en mesure de décrypter. Le surcroît de manipulations qui en résulte pour les utilisateurs en vaut la peine lorsque la confidentialité est prioritaire.

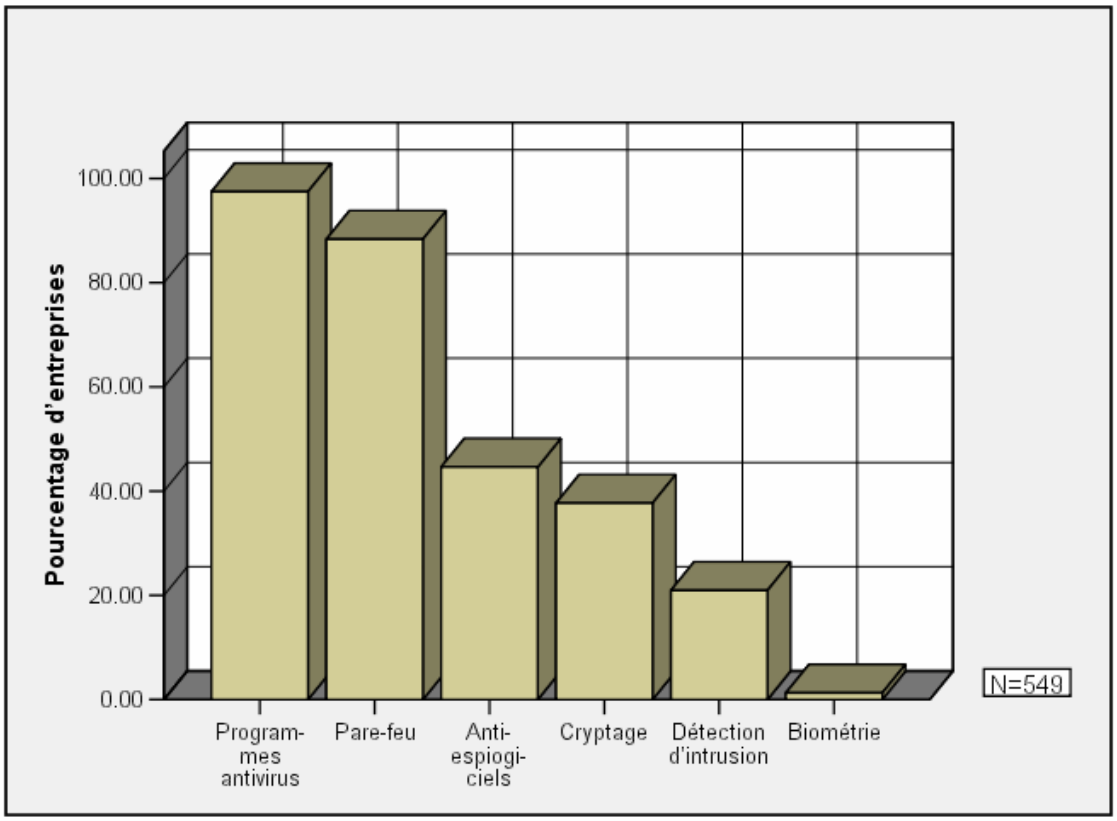
Détection d'intrusion (intrusion detection)
Un système de détection d'intrusion (intrusion detection system, IDS) est un programme qui surveille, enregistre et analyse les activités déployées sur un ordinateur ou sur des réseaux. Des qu'elles s'apparentent à un modèle type d'attaque, le système donne l'alarme. Un bon usage d'un IDS requiert des connaissances bien plus étendues que dans le cas d'un pare-feu ou d'un antivirus.

Mesures biométriques
Ces mesures permettent de limiter l'accès physique aux ordinateurs. L'authentification des utilisateurs reposera par exemple sur ses empreintes digitales, la morphologie de son visage ou la configuration de son iris. De telles procédures coûtent généralement cher.

3.1.2 Utilisation de mesures techniques

La fig. 4 indique la fréquence d'utilisation des mesures susmentionnées dans les entreprises suisses.

Fig. 4 Utilisation des mesures techniques de protection



Globalement presque toutes les entreprises (99,6 % des participants) se protègent avec l'une des mesures techniques présentées. Elles sont d'ailleurs largement plus de 80 % à utiliser à la fois un antivirus et un pare-feu.

Si donc la majorité des entreprises ont pris des mesures techniques élémentaires en matière de sécurité, l'emploi des technologies plus complexes comme la détection d'intrusion et la biométrie est beaucoup moins fréquent. Ce résultat ne surprend guère et correspond assez bien aux résultats des enquêtes du CSI et du FBI à propos des entreprises américaines.[27] Pour des raisons de coûts, on comprend que les entreprises utilisent plus rarement de telles mesures plus exigeantes d'un point de vue aussi bien technique que financier. Pour quelques entreprises elles ne sont d'ailleurs pas judicieuses. Il importe donc d'examiner plus précisément quelles sont les entreprises qui recourent à des mesures plus complexes.

Il s'avère que ce sont avant tout les grandes entreprises qui font usage de telles mesures. A titre d'exemple, 60 % des grandes entreprises recourent aux techniques de cryptage, contre 25 % seulement des micro-entreprises. Si l'on compare différentes branches, on voit bien que ces mesures techniquement sophistiquées sont fréquentes dans l'informatique et le secteur financier essentiellement.[28] Ces résultats étaient à prévoir, dans la mesure où les principales entreprises et en particulier celles du secteur financier ont un réel besoin d'une structure informatique sûre. Quant à la branche informatique, qui possède un important savoir-faire, il n'est guère surprenant qu'elle y recoure pour mettre en place des mesures techniques complexes.

3.1.3 Définition des mesures organisationnelles

Au-delà des mesures techniques adoptées, les entreprises peuvent renforcer leur sécurité de l'information par toutes sortes de mesures organisationnelles. L'enquête portait sur les principales de ces mesures, qui font l'objet ci-dessous d'une brève description.

Politique de sécurité informatique (security policy)
La politique de sécurité informatique d'une entreprise constitue son concept de base pour la sécurité de l'information. Il s'agit de déterminer des objectifs en fonction des besoins de sécurité de l'entreprise, de préciser les responsabilités et de définir les moyens à disposition. La clarté dans ces questions représente la condition nécessaire pour que les différentes unités d'une entreprise collaborent sans accroc sur le plan de la sécurité de l'information.

Gestion des incidents (incident response)
La gestion des incidents consiste à se préparer face aux attaques possibles relevant de la sécurité de l'information. Les mesures à prendre sont d'ordre technique, organisationnel et juridique. Une telle gestion a pour but la reprise aussi rapide que possible de la production informatique après un incident.

27 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), p. 5.

28 63 % des entreprises du secteur financier recourent à des technologies de cryptage, 42 % à la détection d'intrusion et 5 % à des mesures biométriques. Dans la branche informatique, 57 % font appel aux technologies de cryptage, 41 % à la détection d'intrusion et 5 % aux mesures biométriques. Ces entreprises jouent un rôle pionnier dans l'utilisation de ces technologies complexes.

Gestion des sauvegardes (backup)
Les sauvegardes informatiques servent à protéger des pertes de données en tout genre. Une copie des données (*backup*) est ainsi réalisée et gardée en lieu sûr. Lors de l'élaboration d'une gestion des sauvegardes, il s'agit avant tout de déterminer à quelle fréquence les sauvegardes doivent être effectuées, qui en est responsable, quelles sont les données sauvegardées (toutes, les plus importantes, les plus récentes) et comment les copies de données sont elles-mêmes gérées.

Mises à jour et réparation des failles de sécurité (updates / vulnerability scan)
La réelle complexité des systèmes d'exploitation et des applications conduit à la découverte périodique de nouvelles lacunes de sécurité, dont des pirates informatiques ou des maliciels savent profiter. Il est donc crucial de détecter de bonne heure ces lacunes et de les combler à l'aide de programmes correctifs (patches). Les responsabilités sont à préciser, afin que les mises à jour se fassent régulièrement.

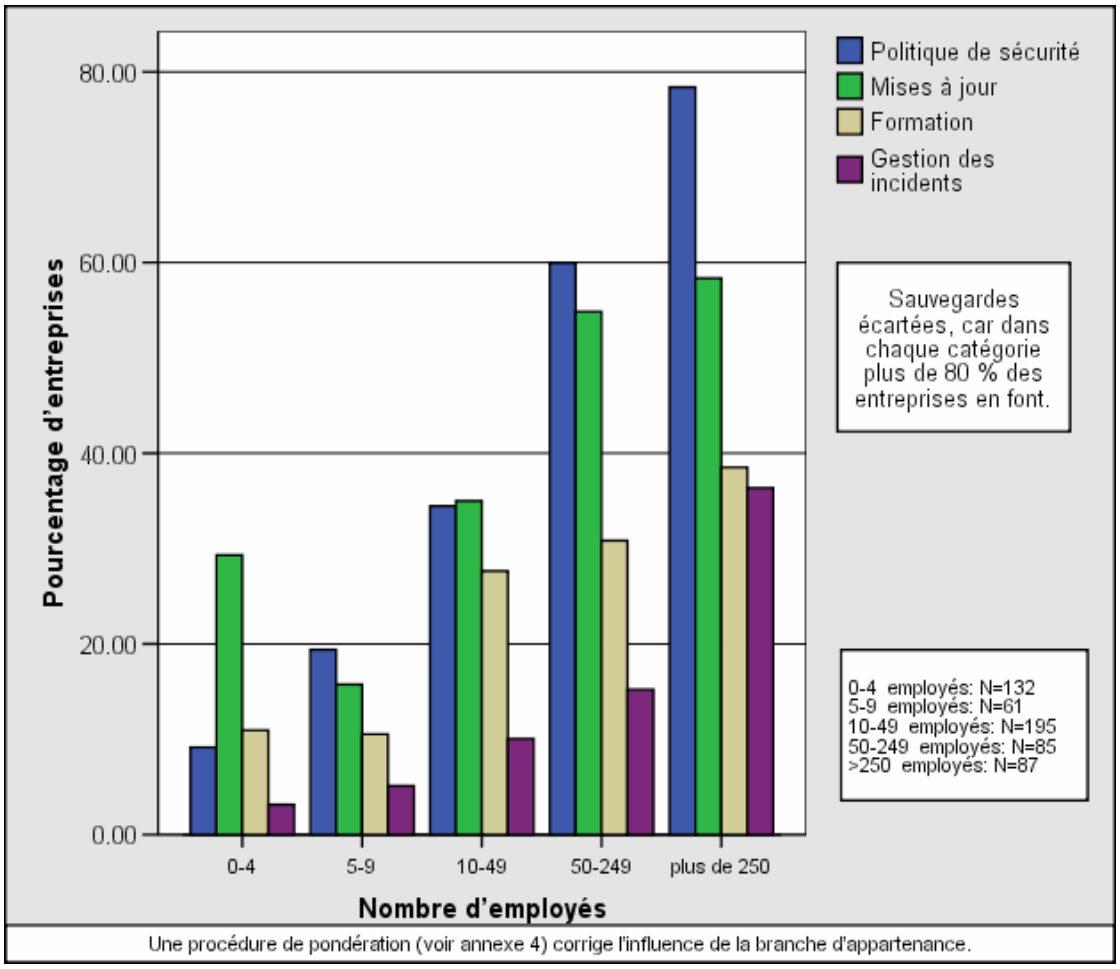
Formation des collaborateurs
Le perfectionnement régulier des collaborateurs dans le domaine de la sécurité de l'information permet de minimiser le risque d'incidents, en corrigeant les comportements fautifs. La formation peut être confiée à des spécialistes externes ou internes, ou se limiter à des campagnes d'information régulières.

3.1.4 Utilisation de mesures organisationnelles

Comme le montre l'analyse de la diffusion des mesures organisationnelles dans les entreprises suisses, la protection des données constitue la préoccupation majeure des entreprises. Presque toutes (91 %) utilisent un concept de sauvegarde. Les autres concepts sont moins utilisés. Quelque 39 % disposent d'une politique de sécurité informatique ou d'une gestion des mises à jour, 26 % forment leurs collaborateurs dans ce domaine et 13 % ont une gestion des incidents.

Là encore, il est intéressant de vérifier si la fréquence d'utilisation des mesures organisationnelles diffère entre les entreprises. La fig. 5 montre le rôle joué par la taille des entreprises.

Fig. 5 Utilisation des mesures organisationnelles selon la taille des entreprises



On voit bien que les mesures organisationnelles apparaissent beaucoup plus souvent dans les grandes entreprises que dans les PME. En effet, il est également plus important pour elles de régler précisément les responsabilités et d'édicter des directives claires pour l'ensemble du personnel. En particulier, la gestion des incidents se développe avec la taille des entreprises. 36 % des grandes entreprises y recourent. Cela montre que par comparaison aux petites entreprises, il est bien plus important pour les grandes entreprises de rétablir l'informatique dans les meilleurs délais après un incident. Pourtant les grandes entreprises sont nombreuses (64 %) à renoncer à la gestion des incidents.

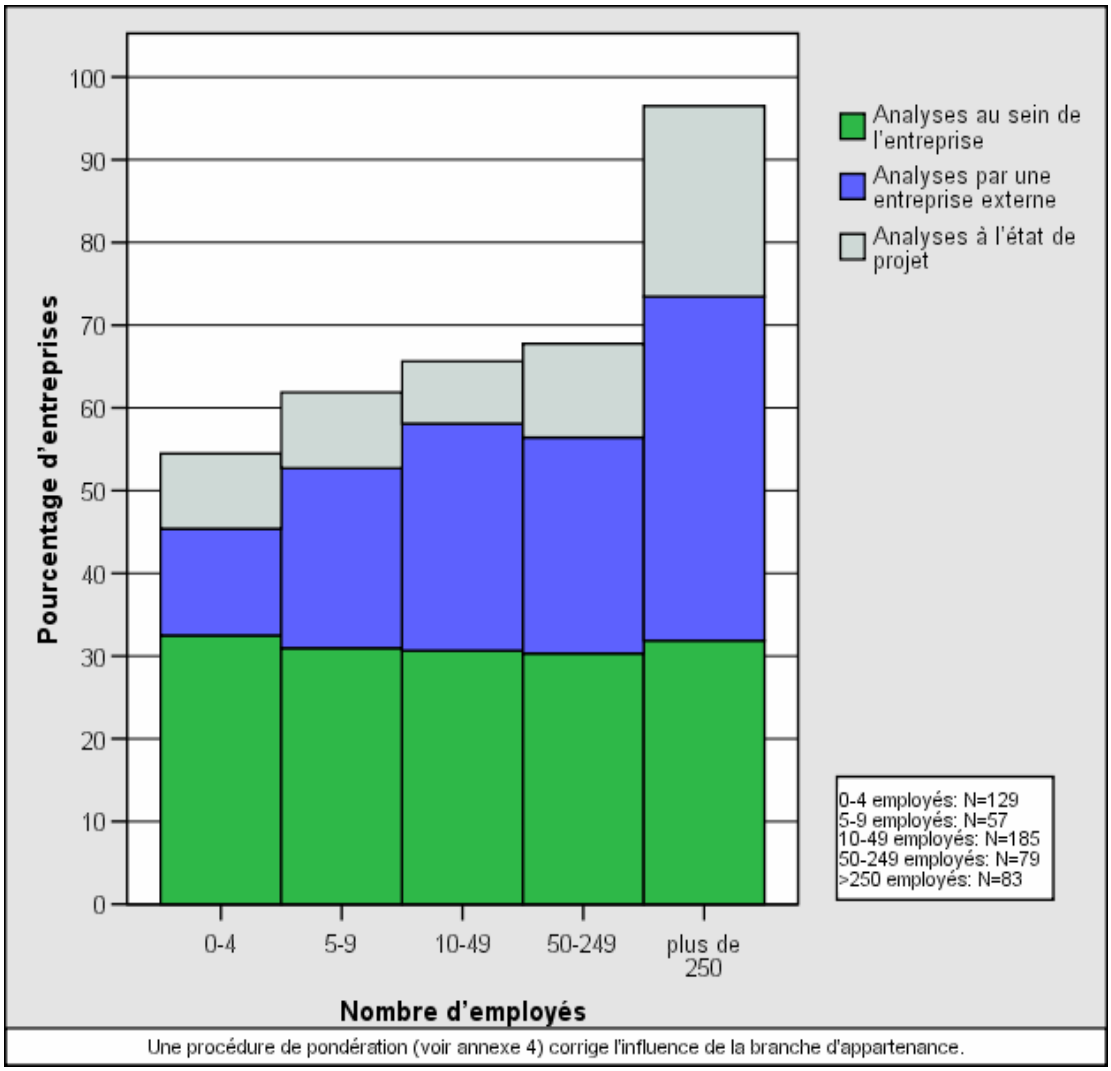
3.1.5 Contrôle des mesures adoptées

Un concept clé de la sécurité, examiné séparément ici, consiste à contrôler en permanence les mesures mises en place. Ce n'est qu'à condition d'analyser fréquemment les mesures destinées à préserver la sécurité de l'information que l'on identifiera de bonne heure les lacunes et pourra réagir avant l'apparition de problèmes. Quelque 56 % des entreprises interrogées procèdent régulièrement à de telles analyses (32 % le font à l'interne et 24 % mandatent une entreprise externe pour les contrôles). En outre, 11 % des enquêtés ont prévu de telles analyses de la sécurité

pour l'avenir.[29] Par contre, un tiers des entreprises ne procède à aucun contrôle régulier ni ne prévoit d'en effectuer à l'avenir.

Là encore, un examen plus détaillé révèle que ce sont avant tout les grandes entreprises qui contrôlent systématiquement leur sécurité. Comme l'indique la fig. 6, quelque 72 % des grandes entreprises procèdent déjà à des analyses de la sécurité et 13 % projettent d'en effectuer.

Fig. 6 Recours aux analyses de la sécurité, selon la taille de l'entreprise



La part élevée des grandes entreprises procédant à des analyses de la sécurité frappe en comparaison des chiffres concernant les entreprises de taille moyenne. Seules les grandes entreprises ont manifestement compris l'importance de revoir régulièrement leurs mesures de sécurité ou disposent des ressources nécessaires à cet effet.

L'étude «Hi-Tech Crime» offre un point de comparaison intéressant avec ces valeurs. Il ressort de cette enquête auprès des sociétés britanniques employant plus 100 personnes que 33 % ne font pas d'analyse de la sécurité.[30] Les grandes entreprises se comportent donc en Suisse, sur le plan des

29 La pondération de ces résultats par la taille de l'entreprise et la branche d'activité (voir annexe 3) permet d'estimer à 47 % la part des entreprises procédant à des analyses de la sécurité. En outre, 8 % planifient pour l'avenir des analyses de la sécurité.

30 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), p. 29.

analyses de la sécurité, comme en Grande-Bretagne (28 % des grandes sociétés helvétiques n'analysent pas leur sécurité pour le moment).

3.2 Charges des entreprises au titre de la sécurité de l'information

Les mesures décrites entraînent parfois des coûts importants. Comme les menaces évoluent en permanence, les entreprises sont tenues d'ajuster constamment leurs mesures techniques et organisationnelles. En outre, le personnel requis doit être mis à disposition et formé. Les entreprises essaient naturellement de réduire au strict minimum leurs coûts liés à la sécurité de l'information. Les charges financières correspondantes sont un bon indicateur pour contrôler l'importance qu'elles accordent à ce paramètre. Il en va de même pour les charges de personnel, pour lesquelles il convient d'examiner non seulement le nombre de collaborateurs, mais aussi le niveau de formation des responsables de la sécurité de l'information.

3.2.1 Charges financières

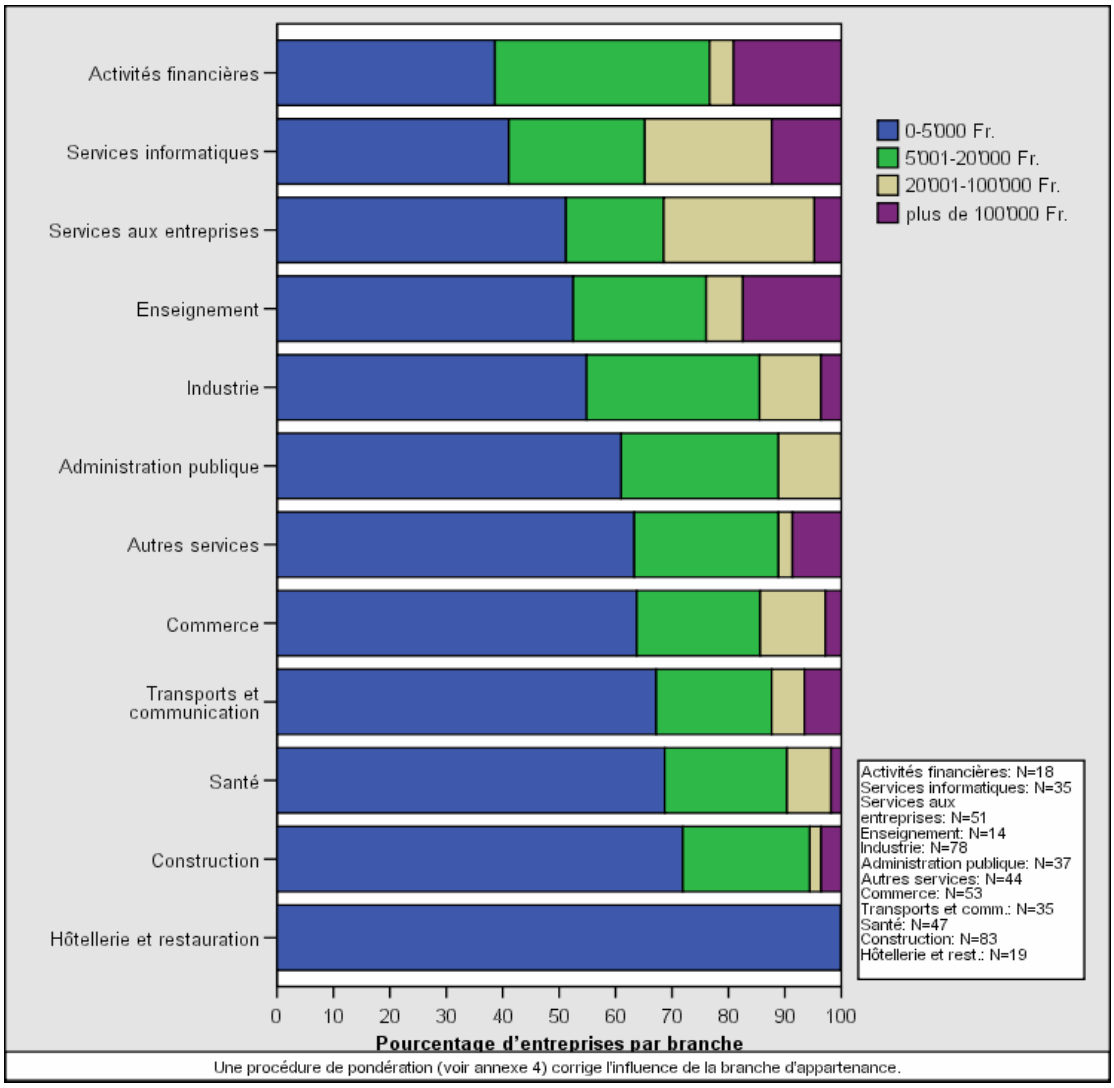
Comme les entreprises sont rares à pouvoir chiffrer précisément leurs coûts liés à la sécurité de l'information, l'enquête distingue quatre catégories (0 à 5000 Fr.; 5001 à 20 000 Fr.; 20 001 à 100 000 Fr.; plus de 100 000 Fr.). L'évaluation montre que beaucoup d'entreprises ont des ressources financières limitées pour assurer leur sécurité de l'information. 62 % de celles qui ont fait état de leurs dépenses n'y consacrent pas plus de 5000 Fr. A l'opposé, seules 5 % consacrent plus de 100 000 Fr. à la sécurité de l'information. Une nouvelle analyse plus détaillée montrera quelles entreprises investissent quels montants pour la gestion des risques.

Le fort lien qui existe entre la taille d'une entreprise et ses charges financières au titre de la sécurité de l'information n'a rien d'étonnant. Plus une société est grande, plus elle investit dans la gestion des risques.[31] Comme leurs budgets sont plus importants, les grandes entreprises disposent de davantage d'argent pour la sécurité de l'information. Ce surcroît de dépenses est certainement justifié, le chapitre qui précède ayant signalé que les grandes société doivent faire face à davantage d'incidents que les PME.

Outre la taille des entreprises, l'activité déployée peut influencer l'engagement financier consenti au titre de la sécurité de l'information. Il a déjà été suggéré, lors de l'étude de la fréquence des incidents par branche, que les entreprises du secteur financier ne sont pas plus touchées que celles de l'hôtellerie-restauration parce qu'elles se protègent mieux des menaces relevant de la sécurité de l'information. La sécurité des données est normalement un enjeu beaucoup plus crucial pour les entreprises du secteur financier que dans l'hôtellerie-restauration. La fig. 7 montre les dépenses consacrées par branche à la sécurité de l'information.

31 Le coefficient de corrélation Gamma exprime la force du lien entre la taille des entreprises et leurs dépenses de prévention. Gamma est compris entre 0 et 1 (max.) pour les corrélations positives. Le rapport étudié ici révèle une valeur élevée (0,791).

Fig. 7 Charges financières liées à la sécurité informatique, par branche



En effet, on constate d'importantes différences entre les branches. Les entreprises des branches susmentionnées constituent les extrêmes. Dans l'hôtellerie-restauration, aucune entreprise ne dépense plus de 5000 Fr. pour la sécurité de l'information, alors que 19 % des entreprises du secteur financier y investissent plus de 100 000 Fr. De façon générale, on peut dire que les entreprises des branches où l'informatique passe pour moins importante limitent logiquement leurs investissements au titre de la sécurité de l'information.

3.2.2 Charges de personnel

L'enquête posait aux entreprises deux questions concernant le personnel et la sécurité de l'information. Il fallait tout d'abord indiquer les charges de personnel, soit le nombre d'emplois en équivalents plein temps,[32] puis le niveau de formation du chef de l'équipe responsable de la sécurité de l'information.

Les réponses sur la taille de l'équipe responsable de la sécurité de l'information révèlent que la plupart des entreprises n'emploient que peu de personnel dans ce but. Dans 13 % des entreprises

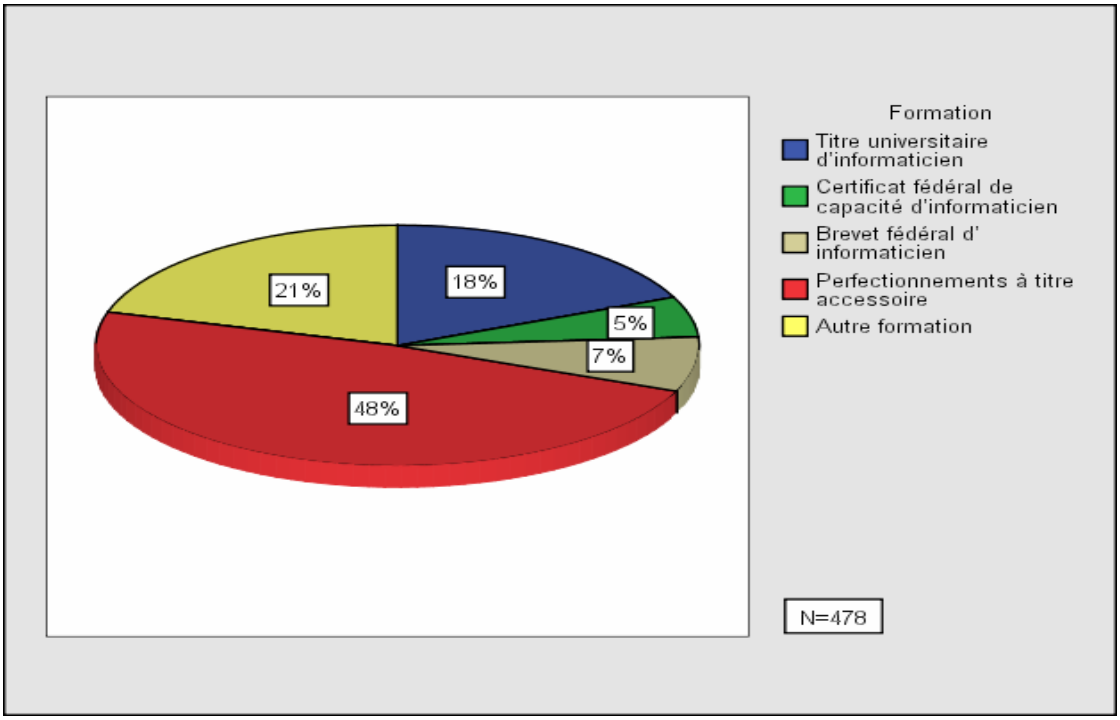
32 Là encore, des catégories étaient proposées pour simplifier: aucun emploi; 0 à 1; 2 à 5; 6 à 10; plus de 10 emplois.

ayant répondu à cette question, aucun employé ne veille directement à la sécurité de l'information. 60 % signalent disposer au maximum de 100 % de poste. Près d'une entreprise sur quatre (24 %) emploie de petites équipes de 2 à 5 collaborateurs, et seules quelques-unes (3 %) occupent plus de cinq personnes dans ce domaine.[33] La sécurité de l'information n'est ainsi que rarement un champ d'activité à part entière dans la politique du personnel des entreprises. Souvent aussi, le manque de moyens financiers fait que les entreprises privilégient des solutions flexibles (conseils externes, externalisation) plutôt qu'une équipe employée.

A l'instar des moyens financiers, les charges de personnel augmentent avec la taille des entreprises.[34] En effet, les grandes entreprises disposent de davantage de collaborateurs et de ressources financières. Néanmoins, ces moyens financiers supplémentaires ne se traduisent pas automatiquement par de plus grandes charges de personnel. L'examen des charges correspondantes par branche d'activité montre en effet que les entreprises du secteur financier ont beau dépenser davantage pour la sécurité de l'information, elles ont tendance à n'occuper que peu de personnel pour ces tâches.[35] Visiblement, certaines branches privilégient les solutions d'externalisation, qui seront analysées plus loin en détail.

Tout d'abord, il s'agit d'étudier encore le niveau de formation des responsables de la sécurité de l'information. Cet aspect compte tout autant que la grandeur de l'équipe pour l'efficacité de la protection. Or les spécialistes coûtent cher et n'offrent qu'une flexibilité limitée d'engagement. Par conséquent, toutes les entreprises ne peuvent pas s'offrir des spécialistes.

Fig. 8 Formation des responsables de la sécurité informatique



33 Là encore, une extrapolation pour toutes les entreprises de Suisse nécessite de corriger la surreprésentation des grandes sociétés et de certaines branches parmi les participants. Une pondération statistique (voir annexe 3) aboutit aux résultats suivants. Dans 22 % des entreprises de Suisse, personne ne s'occupe de la sécurité de l'information, et dans 68 % cette tâche est confiée tout au plus à un employé à plein temps.

34 La force de ce lien s'exprime à nouveau dans le coefficient de corrélation Gamma (voir note 31), qui atteint ici une valeur de 0,588.

35 Comme le montre la fig. 7, les entreprises de la branche financière sont celles qui dépensent le plus pour la gestion des risques. Or moins de la moitié d'entre elles emploient plus de deux spécialistes de la sécurité de l'information.

La fig. 8 montre que dans moins d'une entreprise sur trois, un informaticien qualifié est responsable de la sécurité de l'information. A y regarder de plus près, le pourcentage s'avère même inférieur. En effet, les grandes entreprises et les sociétés de la branche informatique emploient bien plus souvent des informaticiens de formation. Mais si l'on se rappelle que les grandes entreprises sont surreprésentées parmi les sociétés participantes, la part des informaticiens responsables de la sécurité de l'information dans les entreprises suisses tombe à 15 % seulement.[36]

Ce faible pourcentage de spécialistes avec des qualifications formelles devient gênant quand les menaces gagnent en complexité. Or la Suisse ne fait pas exception ici, l'étude britannique «Hi-Tech Crime» déplorant elle aussi le manque de spécialistes avec des qualifications formelles dans le secteur de la sécurité de l'information.[37]

Pour conclure sur la question des charges de personnel dans le domaine de la sécurité de l'information, on peut dire que la plupart des entreprises affectent peu d'employés à cette tâche et que seule une minorité d'entre elles délèguent la responsabilité correspondante à un informaticien qualifié.

3.3 Externalisation des risques

Comme indiqué plus haut, certaines entreprises investissent dans la sécurité de l'information des moyens financiers substantiels tout en y employant peu de personnel. Elles recourent manifestement davantage à des spécialistes externes, ce qui leur offre une flexibilité accrue pour couvrir leurs besoins. L'externalisation n'a toutefois pas que des avantages. En effet, comme à de nombreux égards la protection informatique est davantage une affaire de gestion que de mesures techniques, les tâches touchant à la sécurité de l'information ne peuvent être qu'en partie déléguées. En outre, les spécialistes mis à disposition par les partenaires externes coûtent généralement cher.

Chaque entreprise doit donc trouver la meilleure solution pour elle, entre l'externalisation et la constitution de sa propre équipe, dans le but de garantir la sécurité de l'information. Comme pour de nombreuses entreprises l'externalisation représente un important complément aux mesures internes, le paragraphe ci-dessous en examine la diffusion. Le point qui suit examine si les entreprises s'assurent suffisamment contre les éventuels dommages liés à un incident. Une assurance permet en effet elle aussi d'externaliser le risque, en répercutant les éventuels dommages financiers sur l'assureur.

3.3.1 Fréquence de la collaboration avec des partenaires externes

Pour déterminer l'importance de l'externalisation dans le domaine de la sécurité de l'information en Suisse, les participants à l'enquête étaient interrogés sur le pourcentage des moyens destinés à la sécurité de l'information qui servent à payer des partenaires externes.

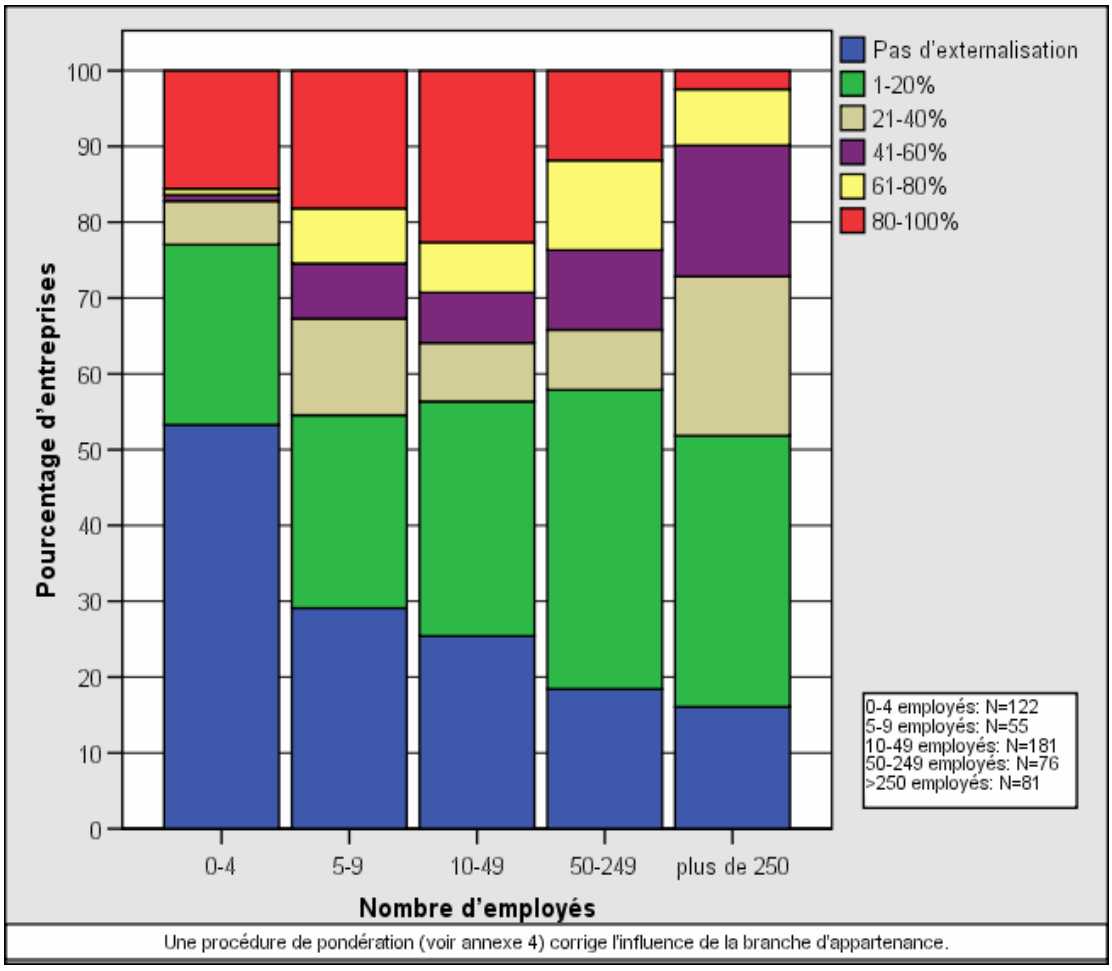
Quelque 30 % des entreprises interrogées ont signalé n'y jamais recourir. En outre, 31 % des entreprises externalisent au maximum 20 % de leurs charges liées à la sécurité de l'information. Autrement dit, plus de la moitié des entreprises ne délèguent qu'une petite partie de leur sécurité de l'information à des spécialistes, tandis qu'à l'autre extrême 15 % des entreprises consacrent plus de 80 % de leurs ressources dans ce domaine à la rétribution de partenaires externes. Les dif-

36 Cette estimation a été obtenue par l'outil statistique de la pondération (voir annexe 3).

37 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), p. 30.

férences d'une entreprise à l'autre sont ainsi considérables. D'où l'intérêt de déterminer quelles entreprises favorisent les solutions externes. La fig. 9 indique la fréquence de l'externalisation en fonction de la taille des entreprises.

Fig. 9 Externalisation en fonction de la taille des entreprises



Les micro-entreprises employant moins de cinq personnes recourent généralement peu à l'externalisation. Ainsi, plus de la moitié d'entre elles se chargent de toute la sécurité de l'information, probablement parce que l'externalisation leur reviendrait trop cher. Les PME ont une attitude très différente, confiant à l'extérieur une part importante de leur sécurité de l'information. Plus d'une entreprise sur cinq comptant 10 à 49 employés externalise au moins 80 % des charges correspondantes. Ces entreprises de taille moyenne dépendent parfois beaucoup de l'informatique, sans avoir la possibilité d'assurer leur sécurité elles-mêmes. Les grandes entreprises au contraire collaborent souvent avec des partenaires externes, mais ne délèguent que très rarement plus de 60 % de leur sécurité de l'information (seules 10 % des grandes entreprises le font).

L'examen de la diffusion de l'externalisation par branche d'activité confirme que les entreprises du secteur financier qui, tout en dépensant beaucoup pour la sécurité de l'information, n'emploient que peu de personnel pour de telles tâches, recourent particulièrement souvent à des partenaires externes. D'un autre côté, il paraît logique que les entreprises de la

branche informatique soient quant à elles peu tentées d'externaliser, étant donné qu'elles possèdent les connaissances nécessaires.[38]

Il n'existe pas d'étude internationale comparable qui permettrait de juger si les entreprises suisses externalisent beaucoup ou peu. Le rôle joué par l'externalisation en Suisse semble certes important en comparaison de la «Computer Crime and Security Survey 2005» du FBI et du CSI. Toutefois, la structure propre aux participants à l'enquête du FBI ne permet pas de comparer directement les résultats.[39]

3.3.2 Couverture par des assurances

Les assurances constituent un cas spécial d'externalisation. En l'occurrence, l'externalisation porte sur les coûts éventuels des dommages liés aux attaques touchant à la sécurité de l'information. En Suisse, des assurances couvrant les risques d'Internet sont proposées depuis 2000 déjà.[40] Les résultats de l'enquête montrent qu'elles se sont imposées très rapidement. Ainsi 45 % des sociétés ayant répondu à la question signalent posséder une assurance contre les dommages susceptibles d'affecter leur infrastructure informatique. Ces indications permettent d'estimer qu'un tiers des entreprises helvétiques ont conclu une telle assurance.[41]

Les entreprises employant de 50 à 249 personnes sont celles qui s'assurent le plus souvent – 69 % d'entre elles ayant conclu une assurance servant à couvrir de tels risques. Le pourcentage est nettement inférieur parmi les micro-entreprises (29 %), et les grandes entreprises sont elles aussi plus rarement assurées (54 %). Par ordre décroissant, on trouve les administrations publiques, suivies des entreprises du secteur financier et des sociétés de services aux entreprises.

Les entreprises ne s'assurant pas invoquent essentiellement des raisons économiques. Ainsi, plus de la moitié d'entre elles (55 %) ont indiqué qu'une assurance n'en valait pas la peine. Par ailleurs 29 % d'entre elles ignoraient l'existence de telles assurances. Enfin, si 15 % ont indiqué ne pas disposer d'argent pour les assurances, 8 % (avant tout des grandes sociétés) jugent insuffisantes les offres des assurances.[42]

A nouveau, il n'existe pas à l'étranger de données comparables sur la couverture des risques par les assurances. Cette absence de possibilité de comparaison n'empêche pas de constater que le taux de pénétration des assurances est étonnamment élevé. Les offres ont beau remonter à quelques années à peine dans ce domaine, de nombreuses entreprises ont déjà conclu une assurance.

38 Dans 9 % seulement des entreprises de la branche informatique, les activités externalisées dépassent 40 % des coûts relatifs à la sécurité de l'information.

39 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), p. 9. Les participants à cette étude du FBI/CSI sont membres du Computer Security Institute (CSI), ce qui suggère qu'ils sont particulièrement actifs dans le domaine de la sécurité de l'information. En outre, l'enquête était ciblée sur les grandes entreprises.

40 Haldemann, Lukas, V*ersicherung von Internet-Risiken* (travail de séminaire au département informatique de l'EPF Zurich, 2001), p. 5.

41 Cette estimation résulte à nouveau d'une pondération des données tirées de l'enquête en fonction de la taille des entreprises et de leur branche d'activité (voir annexe 3).

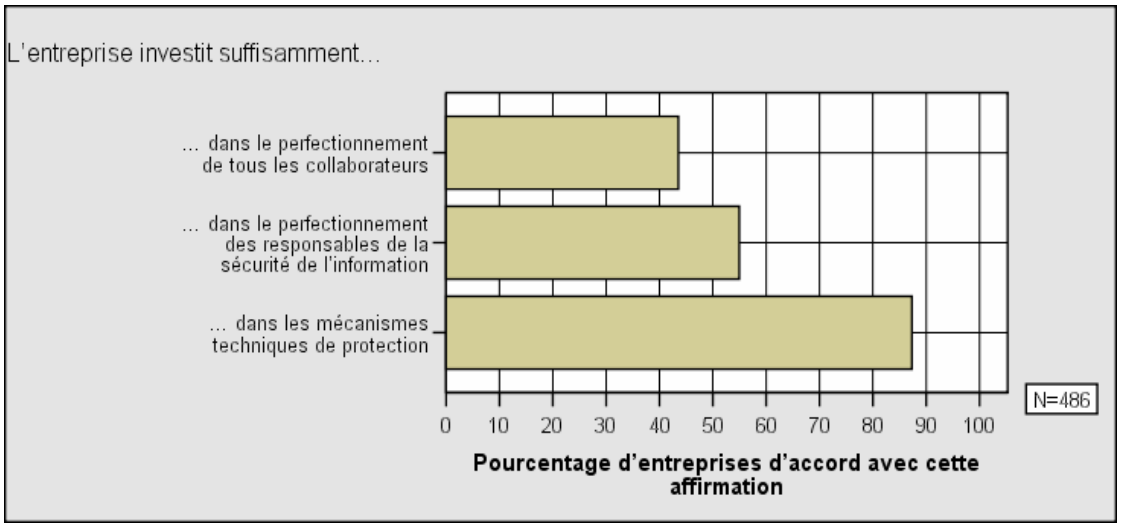
42 Il était permis aux participants de donner plusieurs réponses.

3.4 Bilan de la gestion des risques dans les entreprises

La gestion des risques peut être aménagée de différentes manières. Presque toutes les entreprises utilisent les mesures de sécurité de base (programmes antivirus, pare-feu, sauvegardes). Quelques-unes, les plus petites surtout, s'en tiennent à ces mesures, alors que d'autres ont des besoins de sécurité plus poussés, qu'elles satisfont soit elles-mêmes, moyennant des mesures techniques et organisationnelles supplémentaires, soit avec des partenaires externes. Comme il existe de multiples manières de mettre en place une gestion des risques et qu'elle est parfois définie de façon tout à fait personnalisée, il n'est pas possible d'en évaluer la qualité pour l'ensemble des entreprises. De même, on ne peut mesurer l'effet direct des mesures adoptées sur la probabilité des incidents. Cela tient au fait que les entreprises qui ont pris davantage de mesures courent généralement un risque accru. En outre, ce sont parfois les mesures de protection adoptées qui font découvrir certains incidents.

Les entreprises elles-mêmes paraissent satisfaites des mesures prises. 87 % des participants considèrent que leur entreprise investit suffisamment dans les mesures techniques de sécurité. Mais comme le montre la fig. 10, la satisfaction n'est de loin pas aussi élevée par rapport à la formation. Seule une faible majorité se dit satisfaite de l'engagement des entreprises sur le plan de la formation des responsables de la sécurité de l'information, et une minorité considère que les investissements consentis pour la formation continue des collaborateurs suffisent.

Fig. 10 Evaluation des investissements réalisés dans la sécurité de l'information



La satisfaction qu'affichent les entreprises par rapport à leurs propres investissements ne dit naturellement pas grand-chose de la qualité effective de leur gestion des risques. Néanmoins beaucoup d'entreprises ont clairement reconnu que la sécurité de l'information n'est pas seulement un problème technique, et qu'il faut également investir dans la formation.[43]

A défaut d'un jugement définitif sur la qualité de la gestion des risques, quelques points importants méritent d'être rappelés en cette fin de chapitre:

43 Les résultats correspondent à ceux de l'enquête menée par KPMG sur la satisfaction des responsables des technologies de l'information (chief information officer, CIO) par rapport à la sécurité informatique dans leur entreprise. Cette étude montre un niveau de satisfaction élevé par rapport aux mesures techniques et un faible niveau de satisfaction par rapport à la perception de la sécurité qu'ont les utilisateurs finaux. KPMG, *Gestion de l'informatique 2005* (Zurich et Genève, 2005), p. 26.

Les entreprises suisses externalisent souvent une partie de leur sécurité de l'information (en particulier les entreprises de taille moyenne). Cela tient notamment au fait que le pourcentage de postes prévu pour la sécurité de l'information est généralement très bas, et que fréquemment les collaborateurs ne sont pas des informaticiens de formation. En particulier, les entreprises de taille moyenne sont loin de pouvoir se procurer toutes les mesures dont elles auraient besoin. Au vu des ressources limitées à disposition et en partant de l'idée que beaucoup de responsables auraient besoin de se perfectionner, il importe à présent de déterminer si les entreprises seraient intéressées par des coopérations en matière de sécurité de l'information.

4 Aide externe et coopération

Les chapitres précédents ont montré que la sécurité de l'information est cruciale pour de nombreuses entreprises. La plupart d'entre elles sont régulièrement confrontées à des incidents qui perturbent leurs systèmes informatiques. Pour en venir à bout, une aide externe est souvent nécessaire. Ce chapitre examine d'abord à quelle fréquence les entreprises ont besoin d'aide externe dans de tels cas, puis où elles la trouvent.

Les entreprises se heurtent souvent aux limites de leurs capacités non seulement par rapport aux incidents eux-mêmes, mais aussi par rapport à la gestion des risques. En effet, une protection efficace et efficiente de l'informatique coûte cher et doit être constamment actualisée. Comme beaucoup d'entreprises sont confrontées aux mêmes problèmes, on peut se demander si des échanges réciproques ne seraient pas judicieux. D'où la question de savoir quelles sociétés seraient favorables à une coopération, qui serait en mesure de la coordonner et comment elle serait financée. Le rôle de l'Etat doit également être réexaminé dans cette perspective. La question centrale étant ici de savoir quelles contributions l'Etat serait en mesure de fournir pour soutenir les entreprises dans ce secteur.

4.2 Aide externe en cas d'incident

L'examen de la quote-part des entreprises pratiquant l'externalisation avait permis de constater que les sociétés suisses dépendent souvent de compétences d'autres entreprises sur le plan de la gestion des risques. C'est particulièrement vrai en cas d'apparition d'un incident menaçant la sécurité de l'information. Mais la recherche d'aide peut être délicate pour les entreprises, comme le cas échéant des secrets professionnels risquent d'être divulgués ou l'image de l'entreprise d'être ternie. Par conséquent, la question est de savoir dans quelle mesure les entreprises sollicitent une aide externe en cas de problème touchant à la sécurité de l'information, et à qui elles s'adressent le cas échéant.

Les résultats de l'enquête montrent que 63 % des entreprises ayant constaté un incident sur le plan de la sécurité de l'information ont fait appel à une aide externe.[44] Les entreprises employant 10 à 49 personnes sont celles qui recourent le plus souvent à une aide externe. D'où la confirmation du résultat de l'enquête sur la diffusion de l'externalisation, montrant que les entreprises de cette catégorie sont celles qui s'appuient le plus sur une aide externe. Un coup d'œil à la répartition par branche montre encore que les participants de l'administration publique recourent particulièrement à une aide externe (75 %), alors que conformément aux attentes les entreprises informatiques ont moins souvent besoin de soutien extérieur (36 %).

Il est également intéressant de savoir où les entreprises trouvent l'aide nécessaire. La plupart des sociétés s'adressent à leurs partenaires externes, au fabricant de leurs logiciels ou à leur fournisseur Internet. Néanmoins 40 % d'entre elles signalent qu'elles prennent contact avec des collègues d'autres entreprises, et 25 % se procurent l'aide nécessaire sur Internet.

44 A nouveau ce résultat ne peut être directement transposé à l'économie suisse, puisque les participants à l'enquête ne représentent pas toutes les entreprises dans les mêmes proportions. La procédure de pondération (annexe 3) permet toutefois d'estimer que près de la moitié (47 %) des entreprises suisses concernées par un tel incident sollicitent une aide externe.

Il s'avère ainsi que les entreprises ne recherchent pas toujours l'aide rétribuée d'experts, mais qu'elles s'intéressent aussi aux échanges réciproques de savoirs. Aussi le point qui suit examine-t-il comment l'on pourrait aménager la coopération entre les entreprises.

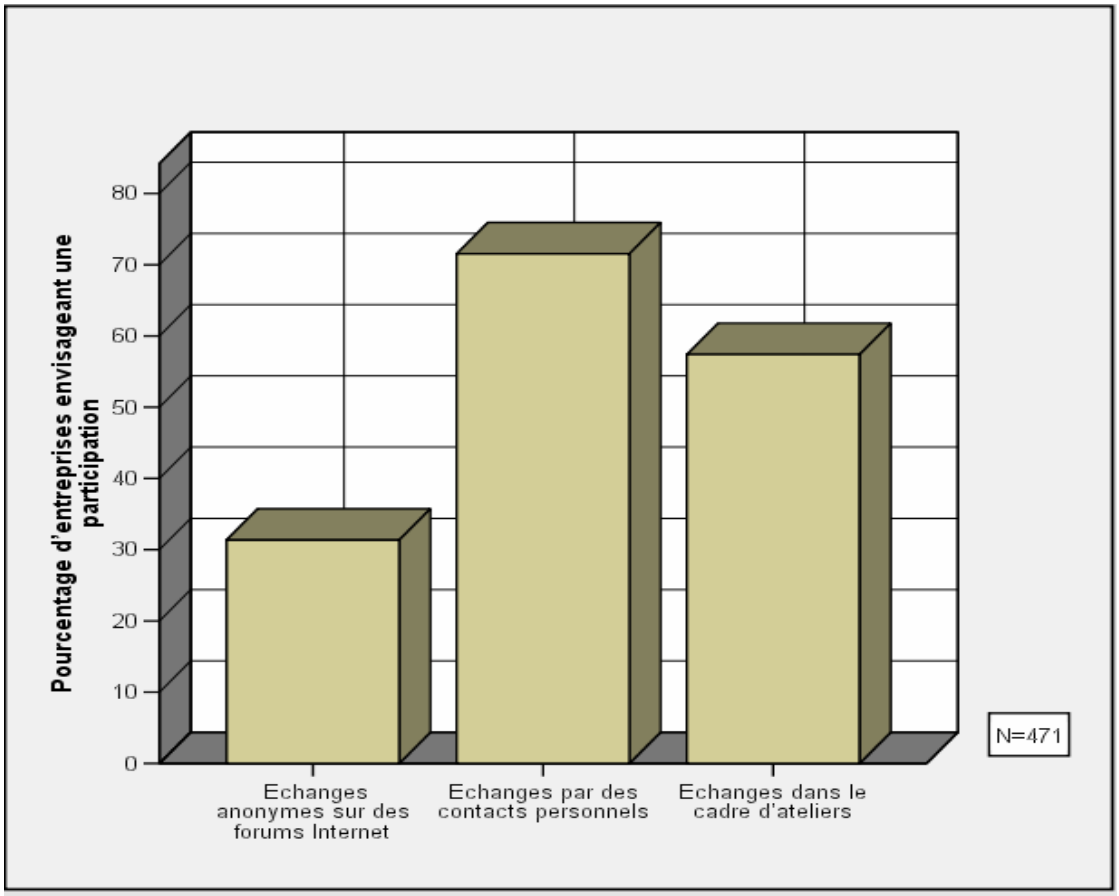
4.2 Coopération parmi les entreprises

Afin d'apprendre quelle collaboration serait judicieuse pour les entreprises, différentes questions doivent être clarifiées. Tout d'abord, il faut déterminer à quelles formes de coopération les entreprises seraient favorables. Puis la question est de savoir qui serait susceptible d'assurer la coordination, et enfin si la volonté est là d'engager des moyens financiers en vue de cette coopération.

4.2.1 Formes possibles de coopération

Pour savoir à quelle collaboration les entreprises consentiraient, les participants à l'enquête ont été interrogés sur la forme de coopération à laquelle ils participeraient. Ils avaient le choix entre les échanges anonymes sur des forums Internet, les échanges entre contacts personnels et les échanges lors d'ateliers. La fig. 11 montre les résultats sur cette question.

Fig. 11 Disposition à collaborer par forme de coopération



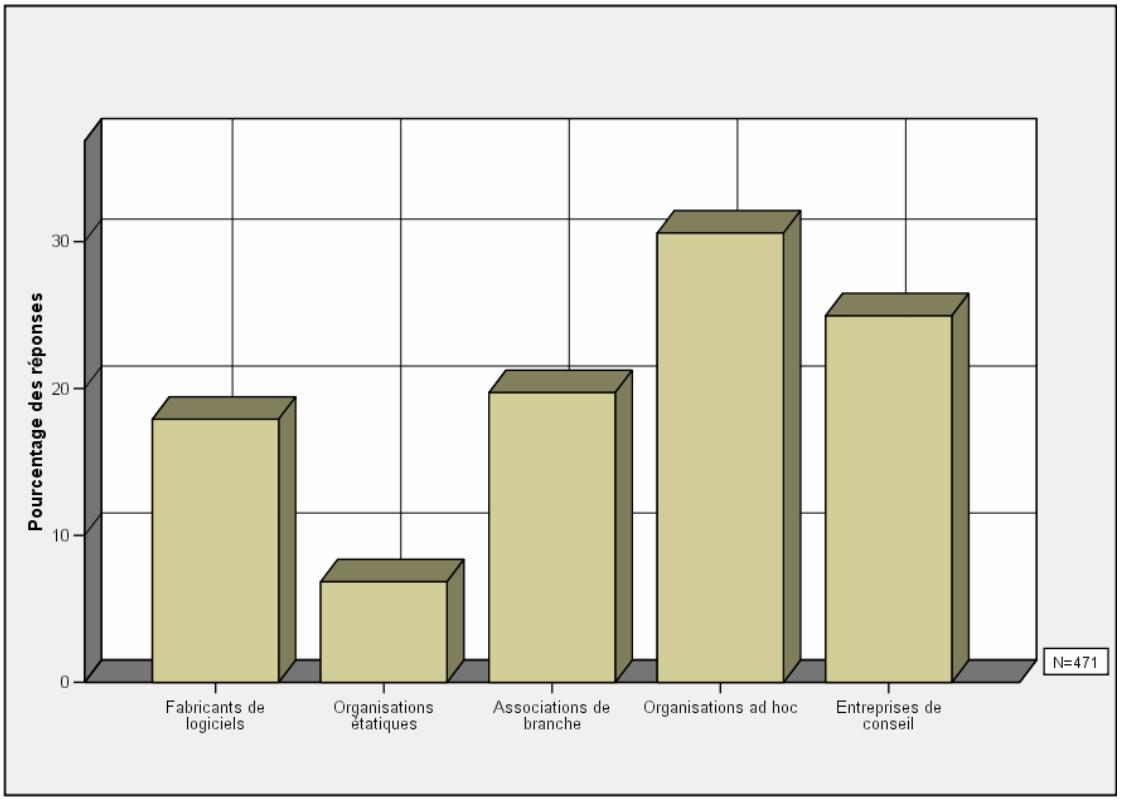
C'est sous la forme des contacts personnels que la volonté de coopération est la plus marquée. Une large majorité participerait volontiers à ce genre d'échanges. L'idée d'ateliers est également bien accueillie.[45] Le réel intérêt qu'inspirent les échanges entre collègues mérite d'être signalé. Les responsables de la sécurité de l'information sont visiblement conscients que beaucoup d'entreprises rencontrent les mêmes problèmes et pourraient ainsi profiter de l'expérience d'autrui. Près du tiers des enquêtés (31 %) se verraient bien discuter via Internet sur les questions relevant de la sécurité de l'information.

Le besoin de coopération est manifeste. D'où l'importance de savoir qui se chargerait le cas échéant de la coordination de la collaboration et si les entreprises envisageraient le cas échéant de fournir une contribution financière à une telle organisation.

4.2.2 Organisation de la coopération

Même si beaucoup d'entreprises souhaitent une collaboration, quelqu'un doit être prêt à en assumer l'organisation. Les entreprises étaient donc invitées à dire qui à leurs yeux serait le plus qualifié comme centre de compétences pour coordonner la collaboration entre entreprises. Les réponses au choix étaient les fabricants de logiciels, les organisations étatiques, les associations de branche, les entreprises de conseil et des organisations spécialement créées à cet effet. La fig. 12 montre l'acteur que les entreprises interrogées préféreraient.

Fig. 12 Organisateurs possibles de la coopération



45 Une distinction a été faite entre les ateliers organisés par les fabricants de logiciels et ceux qui sont organisés par des tiers indépendants. 41 % des entreprises participeraient aux ateliers organisés par les fabricants de logiciels et 50 % aux ateliers organisés par des tiers indépendants. Le graphique prend en compte toutes les entreprises disposées à participer à l'une des deux possibilités.

Ainsi, plus de 30 % des entreprises estiment que la coordination de la coopération serait le mieux assurée par des organisations spécialement créées à cet effet. Il n'y a pas lieu à ce stade d'examiner comment lesdites organisations seraient conçues.

25 % de toutes les entreprises interrogées préconisent sinon de collaborer avec des sociétés de conseil. Les fabricants de logiciels (18 %) ont sans doute été cités parce qu'ils collaborent déjà avec de nombreuses entreprises. Enfin, les associations de branche sont également souvent mentionnées (20 %). L'avantage dans leur cas est qu'elles ont déjà l'expérience de la coordination et de l'organisation des coopérations.

Les plus petites entreprises favorisent les fabricants de logiciels et les entreprises de conseil, tandis que les moyennes ou grandes entreprises indiquent plus souvent les associations de branche et en particulier de nouvelles organisations ad hoc.[46] Les petites entreprises sont sans doute davantage intéressées par des conseils sous forme de mise à disposition de connaissances, alors que les entreprises moyennes ou grandes recherchent plutôt une collaboration avec échange réciproque.

L'exploitation de l'enquête montre en outre clairement que le rôle de conseil et de suivi direct de la coopération n'est pas perçu comme incombant à l'Etat. Le sous-chapitre 4.3 est donc consacré au rôle de l'Etat. Auparavant il sera encore question de la disposition des entreprises à participer financièrement aux coûts d'organisation de la collaboration.

4.2.3 Financement de la coopération

La question du financement de la coopération était formulée en des termes très généraux. Les entreprises devaient dire si elles acceptaient de participer financièrement à concurrence de 500 Fr. ou de 2000 Fr. par an à des organisations chargées d'informer dans le domaine de la sécurité de l'information et de coordonner la collaboration. Ces données visent à traduire la disposition à contribuer aux coûts de la coopération.

Comme la question était formulée de manière vague et que certaines personnes ayant complété le questionnaire n'avaient sans doute pas la compétence nécessaire pour se prononcer sur les engagements financiers de leur employeur, un pourcentage élevé de participants (36 %) n'ont pu y répondre. Parmi ceux qui l'ont fait, 71 % ont signalé qu'ils n'étaient pas disposés à payer, 22 % se sont dits prêts à payer jusqu'à 500 Fr. et 8 % jusqu'à 2000 Fr. Ce sont principalement les grandes entreprises qui seraient disposées à contribuer, dans la mesure où un engagement financier modique pour la coopération dans le domaine de la sécurité de l'information n'affecterait guère leurs budgets. 55 % d'entre elles seraient disposées à contribuer, tandis que seules 15 % des micro-entreprises se verraient payer jusqu'à 500 Fr.

Il n'est guère surprenant qu'une grande majorité refuse toute participation financière, surtout si l'on songe que la plupart des entreprises ont des budgets modestes pour la sécurité de l'information. Néanmoins, plus de la moitié des grandes entreprises et même un tiers des sociétés de 50 à 249 employés consentiraient à participer aux coûts d'une organisation chargée de la collaboration dans le domaine de la sécurité de l'information. Cela montre à nouveau que les moyennes et les grandes entreprises tout au moins souhaitent une coopération renforcée.

46 Les entreprises de moins de 10 collaborateurs préféreraient que la coopération soit organisée par les fabricants de logiciels (29 %) ou par les entreprises de conseil (28 %). Inversement, 43 % des grandes entreprises jugent nécessaire de disposer d'une organisation spéciale.

4.3 Coopération avec l'Etat

Sachant que la sécurité de l'information est un problème qui touche l'ensemble de l'économie, on est amené à se demander si et comment l'Etat peut ou doit soutenir les entreprises dans les mesures de protection qu'elles prennent.

L'une des missions traditionnelles de l'Etat consiste à protéger les infrastructures essentielles au bien-être de sa population. Comme dans les sociétés modernes ce bien-être dépend fortement de la performance des technologies de l'information et de la communication, la protection des TIC est devenue une tâche publique importante. Or l'Etat a besoin du concours des entreprises du secteur privé pour assumer la fonction désignée dans les enceintes internationales comme *Critical Information Infrastructure Protection* (CIIP)[47]. D'où l'intérêt pour lui de coopérer avec les entreprises et de soutenir leurs efforts de protection informatique. Mais à la différence des entreprises, l'Etat poursuit une perspective à plus long terme, qui va au-delà de la simple garantie de l'activité commerciale.

Compte tenu de ces différentes perspectives dans le domaine de la sécurité de l'information, il importe de s'assurer que les entreprises souhaitent collaborer avec l'Etat. Mais comme déjà indiqué, seules quelques entreprises jugent que l'Etat est l'acteur adéquat pour coordonner la coopération entre les entreprises. Elles se montrent donc plutôt critiques sur son rôle. Ces raisons justifient d'examiner jusqu'à quel point l'Etat et les entreprises ont collaboré à ce jour.

4.3.1 Rôle de la police

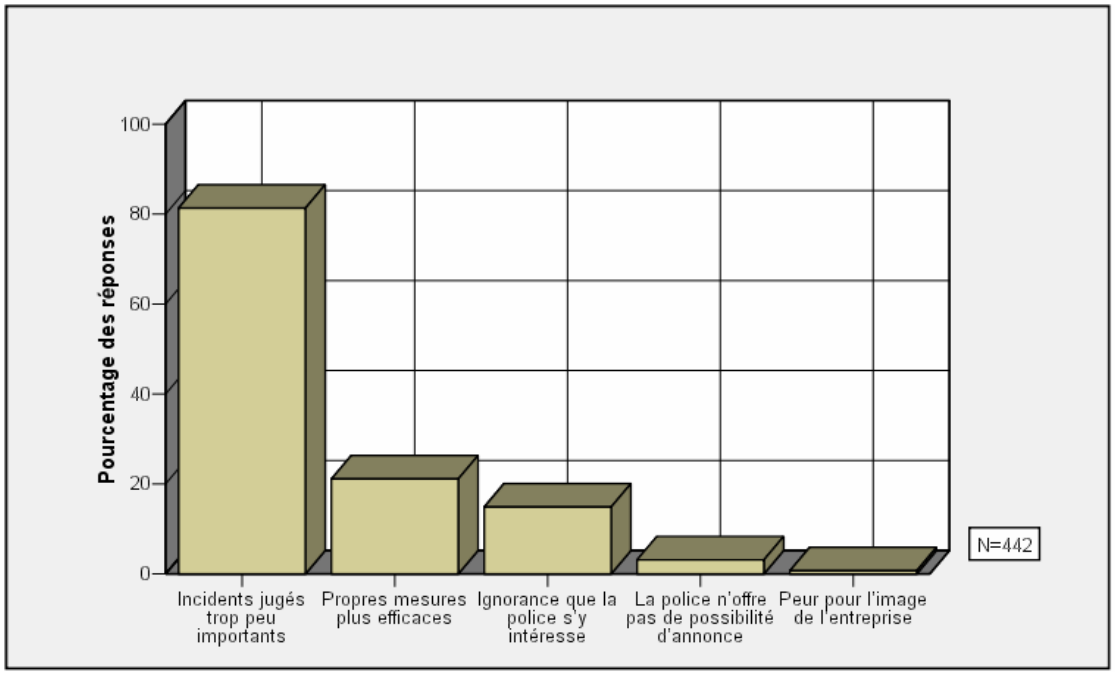
Lorsque des particuliers ou des entreprises sont victimes d'une escroquerie ou d'un vol, ils s'adressent habituellement à la police, chargée de garantir la sécurité contre toute atteinte à la propriété. Or les entreprises font-elles aussi appel à la police lorsque leur infrastructure informatique est attaquée ou qu'elles se font dérober des données?

L'enquête demandait aux entreprises si elles avaient déjà fait appel à la police suite à un incident concernant la sécurité de l'information. Le résultat est net: seules 34 des 562 entreprises interrogées (6 %) ont répondu par l'affirmative. Et parmi ces 34 entreprises, 15 sont de grandes entreprises. Comparaison internationale à l'appui, les entreprises ne préviennent que très rarement la police. L'étude du FBI «Computer Crime Survey» révèle que seules 9,1 % des entreprises américaines s'adressent à la police en pareil cas.

Il est naturellement intéressant de savoir pourquoi ce pourcentage est si bas. Les entreprises ont donc été interrogées sur les raisons pour lesquelles elles n'ont pas prévenu la police. La fig. 13 montre la fréquence des raisons indiquées, les participants ayant la possibilité d'en indiquer plusieurs.

47 Pour en savoir davantage sur la protection des infrastructures critiques en matière d'information, voir: Abele-Wigert, Isabelle et Myriam Dunn, *The International Critical Information Infrastructure Handbook 2006* (Zurich, 2006).

Fig. 13 Raisons pour lesquelles la police n'a pas été prévenue



Un très grand nombre d'entreprises jugent visiblement les incidents trop peu graves pour être signalés à la police. Pour beaucoup, les incidents liés aux maliciels font partie du quotidien et ne sont donc pas annoncés. Il n'est guère surprenant non plus qu'une entreprise sur cinq estime ses propres mesures plus efficaces. En l'occurrence, le comportement de la police n'importe guère ici. Seules quelques entreprises ont indiqué ne pas avoir annoncé l'incident en croyant que la police ne s'intéressait pas à de tels cas ou n'offrait pas la possibilité de les signaler. Il convient également de souligner que contrairement à une opinion très répandue, la peur des dégâts d'image ne dissuade guère les entreprises de faire une annonce.

La comparaison avec l'étude «Computer Crime Survey»du FBI confirme une nouvelle fois ces résultats. Là encore, la principale raison qui amène les sociétés à ne pas prévenir la police est l'idée que les incidents sont trop peu graves.[48]

4.3.2 Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)

Il est très rare que les entreprises jugent bon de faire appel à la police. D'ailleurs les autorités ordinaires de poursuite pénale sont dans l'incapacité de résoudre de nombreux problèmes touchant à la sécurité de l'information. Aussi l'Etat cherche-t-il d'autres formes lui permettant de soutenir l'économie sur le plan de la sécurité de l'information. C'est ainsi que la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a vu le jour. De concert avec les organisations économiques et les autorités, MELANI entend identifier le plus tôt possible les dangers et menaces et offrir aux entreprises la possibilité de lui annoncer les incidents survenus.[49] MELANI est entré en activité le 1er octobre 2004. Son site publie régulièrement des

48 Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005), p. 12.

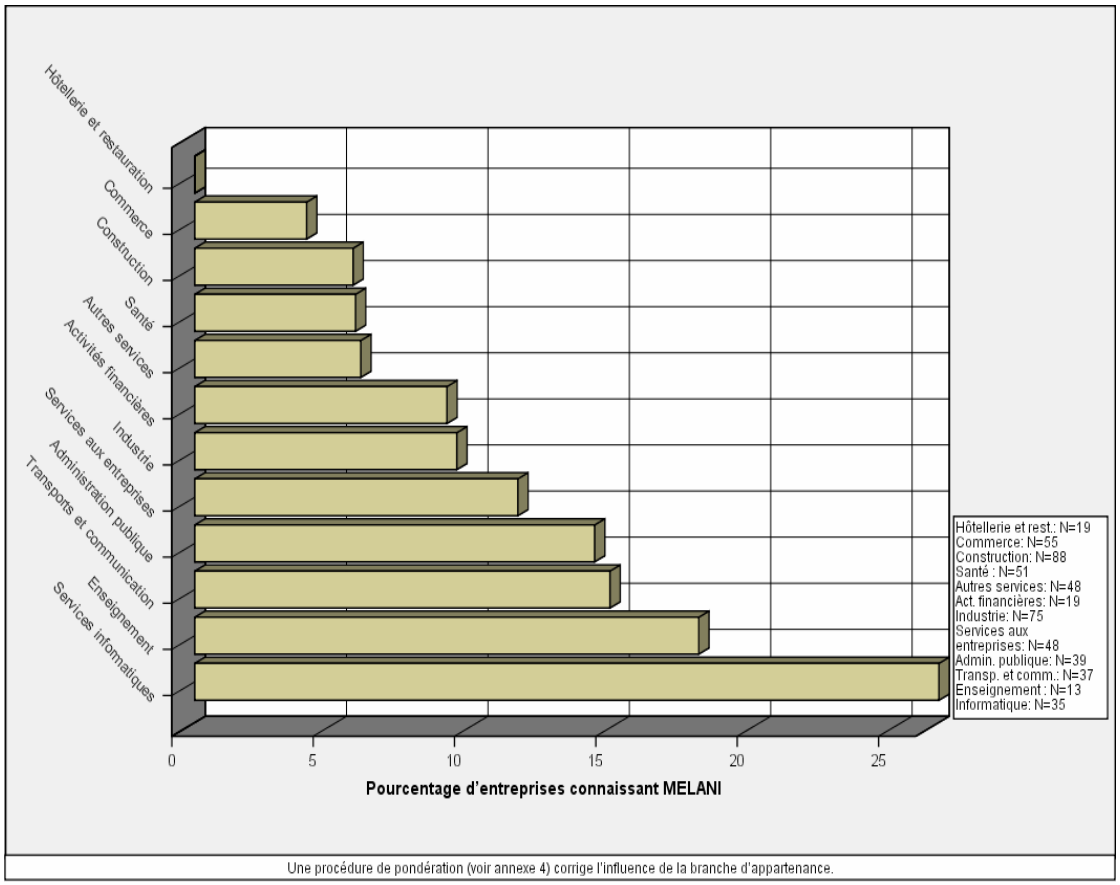
49 Les principaux partenaires sont ici l'Unité de stratégie informatique de la Confédération (USIC), le Service d'analyse et de prévention (SAP) de l'Office fédéral de la police, ainsi que le Computer Emergency Response Team de la fondation Switch (www.switch.ch).

renseignements sur les menaces actuelles et des mises en garde sur les nouveaux dangers.[50] Ces données ne prennent tout leur sens que si les entreprises en tiennent compte. D'où la réelle importance de savoir quel est le taux de notoriété de MELANI parmi les entreprises, après plus d'un an d'activité.

Quelque 10 % des entreprises interrogées connaissent MELANI. Précision utile, MELANI collabore étroitement avec un certain nombre de grands exploitants d'infrastructures critiques, qui n'ont pas participé à l'enquête.

La part des entreprises qui connaissent MELANI augmente en fonction de leur taille. Alors que 4 % seulement des micro-entreprises de moins de 5 employés connaissent MELANI, 28 % des grandes entreprises sont dans ce cas. Comme le montre la fig. 14, on trouve d'importantes différences entre les branches.

Fig. 14 Notoriété de MELANI selon la branche



Les entreprises de la branche informatique sont de loin celles qui connaissent le mieux MELANI. Ainsi MELANI a bénéficié dès l'année de sa création d'une grande notoriété parmi les sociétés s'intéressant à la sécurité de l'information (grandes entreprises et entreprises de la branche informatique).

Comme les problèmes liés à la sécurité de l'information diffèrent fortement (qualité et quantité) selon la taille des entreprises et leur branche d'appartenance, il est difficile pour MELANI de couvrir tous les besoins. Tandis que les grandes entreprises ont besoin de conseils pointus émanant de spécialistes, les entreprises de moyenne taille sont plutôt intéressées par des

50 www.melani.admin.ch.

conseils d'ordre général. Les conclusions de la présente étude examinent de plus près les solutions qui permettraient de résoudre ce problème.

5 Acquis et conclusions

L'étude avait pour but de donner une vue d'ensemble des menaces guettant l'informatique des entreprises suisses ainsi que des moyens de protection existants. Les analyses ont montré que les menaces relatives à la sécurité de l'information sont très répandues et que la gestion des risques dans ce domaine est importante pour toutes les entreprises. Il est non moins clair que la situation est très différente d'une entreprise à l'autre. Ce dernier chapitre aborde les conséquences à tirer des constats qui ont été faits en cours d'étude.

5.1 Diversité des menaces – gestion différenciée des risques – diversité des besoins

La première conclusion importante de l'étude est que les menaces en matière de sécurité de l'information varient considérablement d'une entreprise à l'autre. Si la branche d'activité a une influence, la taille des entreprises semble plus importante encore. En effet, alors que les PME sont surtout victimes des maliciels, une grande entreprise sur cinq a constaté en 2005 une attaque ciblée sur son infrastructure informatique. D'où l'importance de distinguer, pour l'évaluation des résultats, entre les grandes entreprises, les exploitations de moyenne taille et les micro-entreprises.

5.1.1 Micro-entreprises

Les micro-entreprises comptant moins de cinq employés sont le moins exposées aux menaces portant sur la sécurité de l'information. Leur exploitation dépend souvent moins fortement de l'informatique que dans le cas des grandes entreprises, et elles ne représentent généralement pas une cible attrayante pour les pirates. Par conséquent, la priorité pour elles est d'adopter une protection de base. Les mesures techniques complexes et les concepts de sécurité approfondis n'ont souvent guère d'utilité pour elles. Il s'ensuit que les plus petites entreprises jouissent d'une relativement grande autonomie dans le domaine de la sécurité de l'information – étant en mesure de réaliser elles-mêmes ce qui est nécessaire. Les recommandations pratiques, le cas échéant des formations, seraient en revanche très précieuses car les micro-entreprises n'emploient généralement pas d'informaticien.

5.1.2 Moyennes entreprises

A la différence des plus petites entreprises, l'informatique est déjà un facteur d'organisation capital pour les moyennes entreprises. Elles sont souvent tributaires d'une infrastructure informatique performante. D'où naturellement un besoin de sécurité croissant dans ce domaine. La protection technique contre les maliciels ne suffit plus, il faut élaborer des concepts et instruire le personnel. Pourtant les moyennes entreprises sont généralement trop petites pour embaucher des spécialistes responsables de la sécurité de l'information. Il n'est donc guère étonnant qu'elles soient les plus demandeuses d'un appui dans le domaine de la sécurité de l'information. Elles collaborent particulièrement souvent avec des partenaires externes, elles sont le plus susceptibles de s'assurer et sollicitent très souvent une aide externe en cas d'incident. Comme beaucoup de moyennes entreprises n'ont pas d'informaticien alors qu'elles doivent mettre en place des mesures

de protection complexes, une offre de cours, de la formation continue et des plate-formes d'échange d'expérience leur rendraient un grand service.

5.1.3 Grandes entreprises

Les grandes entreprises ont d'autres besoins encore. Comme leur informatique est particulièrement menacée, elles doivent se doter de mesures de protection sophistiquées. Elles y affectent davantage de moyens financiers et de personnel, adoptent des mesures techniques plus complexes et introduisent plus souvent des concepts de sécurité. Du fait des attaques ciblées plus nombreuses dirigées contre elles, elles sont exposées à des menaces bien plus sérieuses. Les méthodes des pirates évoluent rapidement, et il s'agit d'être toujours à jour. Les spécialistes et les équipes d'informaticiens internes sont néanmoins rapidement confrontés à leurs limites.

Les grandes entreprises sont donc particulièrement intéressées par les conseils spécifiques émanant de spécialistes. En effet, au-delà des simples questions générales concernant la sécurité, il leur faut mettre concrètement en œuvre des mesures plus complexes et techniquement délicates. Ces entreprises sont de surcroît interconnectées et dépendent souvent les unes des autres. D'où la nécessité, en plus des conseils, d'organiser et d'encourager la coopération et les échanges réciproques. Les grandes entreprises peuvent d'ailleurs être très intéressées à collaborer avec la police en cas d'attaque portant sur la sécurité de l'information.

Les souhaits des grandes entreprises diffèrent ainsi nettement de ceux des PME. Leurs besoins de conseils spécifiques et de coopération sont toutefois connus depuis plus longtemps, et les possibilités de collaboration étroite avec MELANI en tiennent compte. Une coopération très active ne peut toutefois être proposée qu'à un cercle restreint de grandes entreprises, pour des raisons de coûts et de ressources.

5.2 Coopération différenciée: structures locales (Warning, Advice and Reporting Points, WARP)

Un deuxième acquis important de l'étude est que les entreprises actives dans la sécurité de l'information collaboreraient volontiers davantage. Beaucoup de sociétés sont confrontées à des difficultés analogues et profiteraient de tels échanges d'expérience. Le problème concernant la mise en œuvre de la coopération tient au fait que comme indiqué plus haut, les diverses entreprises ont des besoins très différents.

Une solution possible à ce problème pourrait résider dans la création de structures locales (Warning, Advice and Reporting Point, WARP). Le centre de coordination de la sécurité des infrastructures nationales du gouvernement britannique (NISCC) favorise de telles initiatives, constituant une plateforme idéale pour les échanges et la collaboration dans le domaine de la sécurité de l'information.[51] Les membres des WARP échangent des informations et combattent ensemble les menaces pesant sur la sécurité de l'information, ce qui favorise l'identification précoce des nouvelles menaces et la mise à disposition de solutions possibles à tous les membres. Il est décisif que les WARP puissent être constitués selon les besoins des entreprises de la même branche, d'une région donnée ou de taille comparable. Les WARP amènent des entreprises éprouvant le même genre de problèmes et des besoins analogues à coopérer entre elles. Les résultats de l'étude indiquent que la taille des entreprises devrait être un critère essentiel dans la conception de

51 www.niscc.gov.uk/niscc/warpInfo-en.html.

WARP. Car si les grandes entreprises sont principalement intéressées par les conseils spécifiques de professionnels, les PME ont besoin de conseils généraux et d'échanges réciproques. Les WARP seraient d'autant plus adéquats dans le cas des moyennes entreprises que la coopération avec des entreprises comparables leur permettrait d'améliorer leur sécurité de l'information, sans qu'il leur en coûte cher.

L'Etat pourrait donner l'impulsion aux WARP et les coordonner dans la phase initiale. Son appui risque même d'être nécessaire, étant donné la tendance des entreprises à participer à de telles organisations une fois seulement que la preuve de leur avantage a été faite. La coordination entre WARP serait également importante, en conduisant à créer des interfaces utiles. Ainsi, tandis que les entreprises faisant partie de WARP spécialisés s'efforceraient de préserver leur activité commerciale, l'Etat encouragerait la sécurité de l'économie en général – comme le veut sa mission en matière de politique de sécurité – en veillant à la coordination de ces organisations.

6 Bibliographie

Abele-Wigert, Isabelle et Myriam Dunn, The International Critical Information Infrastructure Protection (CIIP) Handbook 2006. An Inventory and Analysis of Protection Policies in Twenty Countries (Zurich, 2006).

Bidgoli, Hossein et al. (éd.), Handbook of Information Security Volume 1-3 (Hoboken, 2006).

Bundesamt für Sicherheit für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2005 (Juli 2005). www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf

Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), 2005 Computer Crime and Security Survey (2005). www.gocsi.com

Dübendorfer, Thomas, Arno Wagner et Bernhard Plattner, An Economic Model for Large-Scale Internet Attacks (étude du Computer Engineering and Networks Laboratory de l'EPF Zurich, 2004). www.tik.ee.ethz.ch/~ddosvax/publications/papers/WETICE-ES-duebendorfer-economic_damage_model.pdf

Eckert, Claudia, IT-Sicherheit: Konzepte – Verfahren – Protokolle (3e éd. remaniée et complétée, Munich et Oldenbourg, 2004).

Federal Bureau of Investigation (FBI), 2005 FBI Computer Crime Survey (2005). www.fbi.gov/publications/ccs2005.pdf

Gartner Research, Enterprises and Employees: The Growth of Distrust (2005). www.csoonline.com/analyst/report3317.html (résumé des résultats)

Haldemann, Lukas, Versicherung von Internet-Risiken (travail de séminaire au département informatique de l'EPF Zurich, 2001). www.ifi.unizh.ch/ikm/Vorlesungen/inf_recht/2001/Haldemann.pdf

KPMG, Gestion de l'informatique 2005: Point de la situation et tendances de l'informatique en Suisse (Zurich et Genève, 2005).

Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), Sûreté de l'information. Situation en Suisse et sur le plan international. Rapport semestriel 2005/1 (2005). www.melani.admin.ch/berichte/lageberichte/index.html?lang=fr#sprungmarke0_3

Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), Sûreté de l'information. Situation en Suisse et sur le plan international. Rapport semestriel 2005/2 (2006). www.melani.admin.ch/berichte/lageberichte/index.html?lang=fr#sprungmarke0_3

National Hi-Tech Crime Unit (nhtcu), Hi-Tech Crime: The Impact on UK Business 2005 (2005).www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

Sieber, Pascal, Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002 (étude réalisée sur mandat du Secrétariat d'Etat à l'économie, Berne, 2002).

7 Annexe

Annexe 1: Structure de l'échantillon / Classification des entreprises

- L'**objet d'étude comprenait toutes les entreprises** du secteur secondaire et du secteur tertiaire.
- Les grandes entreprises faisant partie du réseau MELANI-Net ont été exclues.
- L'enquête visait à réunir au moins 500 participants. Le taux de retours était estimé à 10 % des entreprises interrogées. D'où l'objectif de constituer un **échantillon de 5000 entreprises**.

- **Critères servant à distinguer les entreprises:**
  a) **Taille:**
     - plus petites entreprises (micro-entreprises): 0 à 4 emplois à plein temps
     - petites entreprises: 5 à 9 emplois à plein temps
     - moyennes entreprises: 10 à 49 emplois à plein temps
     - grandes entreprises: 50 à 249 emplois à plein temps
     - plus grandes entreprises: plus de 250 emplois à plein temps

  b) **Branches** selon la systématique des branches économiques de l'Office fédéral de la statistique.[52]
     - **Industries manufacturières:** unités engagées dans la transformation mécanique, physique ou chimique de matériaux, substances ou composants en nouveaux produits.
     - **Construction:** bâtiments et ouvrages de génie civil, installations du bâtiment et travaux de finition.
     - **Commerce:** commerce de gros ou de détail (vente sans transformation) de tout type de marchandises, avec la prestation de services liés à la vente de marchandises.
     - **Hôtellerie et restauration:** mise à disposition de lieux d'hébergement et/ou de repas préparés, produits apéritifs et boissons pour consommation immédiate.
     - **Transports et communications:** activités liées au transport, régulier ou non, de passagers et de marchandises par rail, par conduites, par route, par eau ou par air.
       Activités auxiliaires telles que la gestion d'installations de terminaux et de stationnement, la manutention du fret, l'entreposage, etc., activités de poste et de télécommunications. Location de matériel de transport avec chauffeur ou opérateur.
     - **Activités financières:** activité d'obtention et de redistribution de fonds à des fins autres que le financement de la sécurité sociale obligatoire ou des caisses d'assurance ou de retraite.
     - **Services aux entreprises:** activités qui visent essentiellement le secteur des entreprises. Or plus ou moins toutes les activités couvertes par cette section peuvent avoir pour destinataires des ménages privés également, par exemple: la location de biens ménagers et personnels, les activités des bases de données, les services

52 NOGA: Nomenclature Générale des Activités économiques. Des précisions sur cette systématique figurent sur le site de l'Office fédéral de la statistique:
www.bfs.admin.ch/bfs/portal/de/index/infothek/nomenklaturen/blank/blank/noga0/publikationen.html

juridiques, les services de recherche et de sécurité, la décoration intérieure ou les activités photographiques.

- **Services informatiques:** activités liées au matériel et aux logiciels informatiques et au traitement usuel des données.
- **Administration publique:** activités habituellement exercées par l'administration publique. Le statut légal ou institutionnel n'est pas, en soi, le facteur déterminant.
- **Enseignement:** enseignement, public ou privé, de tous les degrés et dans toutes les disciplines, délivré par les différentes institutions composant le système scolaire traditionnel, mais aussi l'enseignement pour adultes, les programmes d'alphabétisation, etc.
- **Santé:** hôpitaux, cabinets médicaux, activités vétérinaires, action sociale (dont maisons pour personnes âgées, homes médicalisés, foyers pour enfants et adolescents).
- **Autres services:** services n'étant pas destinés en premier lieu à des entreprises (p. ex. culture, sport, blanchisseries, salons de coiffure et instituts de beauté, etc.).

- **Plan de l'échantillon:**
  L'échantillon devait être structuré de façon à permettre des commentaires sur différentes tailles d'entreprises et pour les différentes branches. Le choix s'est donc porté sur un modèle d'échantillon disproportionnel (quota random). Il a fallu ensuite corriger toutes les classes sur- ou sous-représentées, ce qui a nécessité une nouvelle correction sous forme de pondération. Dans les nombreuses branches ne possédant que peu de grandes sociétés, il a fallu recenser toutes les entreprises de la catégorie de plus de 250 collaborateurs.
  Les adresses des entreprises ont été demandées à l'Office fédéral de la statistique selon le plan d'échantillonnage suivant:

Quotes-parts à respecter pour la commande des adresses

Sous-sections NOGA (divisions)	Catégories de grandeur (EPT)		
	0-9	10-249	250+
D Industrie manufacturière (15-37)	330	420	250
F Construction (45)	300	390	tous
G Commerce (50-52)	500	400	100
H Hôtellerie et restauration (55)	220	320	tous
I Transports et communications (60-64)	200	200	tous
J Activités financières et assurances (65-67)	120	160	tous
K Activités immobilières et services aux entreprises (70-74)	550	350	tous
L Administration publique, défense, assurances sociales (75)	60	130	tous
M Education et enseignement (80)	140	210	tous
N Santé, affaires vétérinaires et action sociale (85)	270	220	100
O Autres services à des tiers (90-93)	310	200	tous
Total	**3'000**	**3'000**	**~1000**

EPT = équivalents plein temps
tous = enquête exhaustive

- Une réserve de 2000 adresses a été constituée. L'enquête a été envoyée à 5000 entreprises. Mais comme certaines adresses n'étaient plus valables, la taille effective de l'échantillon était de 4916 entreprises.

Annexe 2: Retours

- 562 entreprises ont participé à l'enquête, soit un **taux de retours** de **11,45 %**.
- Il n'y a pas eu d'analyse systématique de la **non-participation**. Mais comme dans chaque enquête où seule une partie des personnes contactées remplissent le questionnaire, le risque existe que les participants diffèrent de la moyenne dans des secteurs significatifs. On pourrait ainsi penser que le simple fait de participer à l'enquête est déjà un indice montrant qu'une entreprise s'intéresse plus à la sécurité de l'information que d'autres. Les entreprises ayant motivé leur abstention donnent une idée des raisons de la non-participation. Sur les **44 refus motivés**, l'absence d'intérêt ou le manque de temps ont été invoqués une fois sur deux. 8 entreprises ont indiqué ne pas utiliser l'informatique, 10 autres ont déclaré ne pas être compétentes pour répondre aux questions, et 4 entreprises se sont abstenues de répondre pour des questions de sécurité.

  Retours selon la taille de l'entreprise:

Taille	Nombre	en %
0-4	132	23,49
5-9	62	11,03
10-49	195	34,70
50-249	86	15,30
>250	87	15,48

Retours par branche:

Branche	**Nombre**	**en %**
Industrie	82	14,59
Construction	92	16,37
Commerce	59	10,50
Hôtellerie et restauration	20	3,56
Transports et communic.	37	6,58
Activités financières	21	3,74
Services aux entreprises	53	9,43
Services informatiques	37	6,58
Administration publique	42	7,47
Enseignement	14	2,49
Santé	56	9,96
Autres services	49	8,72

Annexe 3: Pondération des données

- **Les participants à l'enquête ne reflètent pas la réalité en ce qui concerne la taille des entreprises et les branches d'appartenance**. En effet, alors que seules 0,3 % des entreprises emploient plus de 250 collaborateurs, elles représentent 15 % des participants à l'enquête. Quant aux branches, les entreprises de la construction sont surreprésentées, tandis que les sociétés de services aux entreprises ainsi que l'hôtellerie et la restauration sont sous-représentées.
- Cette représentation non proportionnelle de la réalité était néanmoins indispensable afin d'obtenir suffisamment de données pour une comparaison. En revanche, elle ne permet pas de tirer directement, à partir des observations faites sur la moyenne des participants, des conclusions valables pour toutes les entreprises suisses du secteur secondaire et du secteur tertiaire.
- Une pondération des données s'impose afin d'obtenir malgré tout des estimations pour toutes les entreprises de Suisse.
- La pondération effectuée signifie que **toutes les données** sont **multipliées par le facteur de pondération w**, lequel se calcule comme suit:

$$w = \frac{n_{Ri}/N_R}{n_{Si}/N_S}$$

n_{Ri}= nombre d'entreprises de la catégorie i dans la réalité
N_R= nombre d'entreprises dans la réalité
n_{Si}= nombre d'entreprises de la catégorie i dans l'échantillon
N_S= nombre d'entreprises dans l'échantillon

- Au total, il convient de distinguer 60 catégories (5 classes de grandeur et 12 branches différentes). Le facteur de pondération w peut être calculé pour chaque catégorie, en divisant le pourcentage des entreprises existantes par leur pourcentage dans l'échantillon.

Branche	Total (réalité)	Total (enquête)	Pondération	0-4 (r)	0-4 (e)	Pond.	5-9 (r)	5-9 (e)	Pond.
Industrie	12.82	14.64	0.88	8.17	1.43	5.72	1.86	0.71	2.61
Construction	10.91	16.43	0.66	7.11	2.50	2.85	1.88	3.39	0.55
Commerce	22.60	10.54	2.14	17.36	3.21	5.41	3.08	1.07	2.88
Hôtellerie et restauration	7.91	3.39	2.33	5.02	0.36	13.96	1.74	0.36	4.85
Transports et communication	3.50	6.61	0.53	2.53	1.61	1.57	0.43	0.54	0.79
Activités financières	1.71	3.75	0.46	1.07	0.89	1.20	0.25	0.00	
Services aux entreprises	19.39	9.46	2.05	16.39	3.21	5.11	1.78	1.25	1.43
Services informatiques	3.52	6.61	0.53	2.90	3.04	0.95	0.30	0.54	0.56
Administration publique	0.74	7.50	0.10	0.29	0.89	0.32	0.11	0.89	0.13
Enseignement	2.21	2.50	0.89	1.28	1.07	1.20	0.25	0.00	
Santé	6.87	9.82	0.70	5.29	2.32	2.28	0.69	0.89	0.78
Autres services	7.83	8.75	0.89	6.64	3.04	2.18	0.69	1.25	0.55
Total	100.00	100.00		74.06	23.49		13.08	11.03	

Branche	10-49 (r)	10-49 (e)	Pond.	50-249 (r)	50-249 (e)	Pond.	250+ (r)	250+ (e)	Pond.
Industrie	2.06	4.64	0.44	0.60	3.93	0.15	0.13	3.93	0.03
Construction	1.68	7.32	0.23	0.22	2.32	0.10	0.02	0.89	0.02
Commerce	1.84	4.64	0.40	0.26	0.54	0.48	0.05	1.07	0.05
Hôtellerie et restauration	1.03	2.14	0.48	0.10	0.36	0.28	0.01	0.18	0.05
Transports et communication	0.43	2.68	0.16	0.09	0.89	0.10	0.02	0.89	0.02
Activités financières	0.30	0.54	0.55	0.06	0.18	0.34	0.03	2.14	0.02
Services aux entreprises	1.05	2.32	0.45	0.14	1.79	0.08	0.02	0.89	0.02
Services informatiques	0.27	1.96	0.14	0.04	0.36	0.11	0.01	0.71	0.01
Administration publique	0.21	1.79	0.12	0.09	1.79	0.05	0.03	2.14	0.01
Enseignement	0.49	1.07	0.46	0.16	0.18	0.91	0.02	0.18	0.14
Santé	0.59	2.86	0.20	0.25	1.96	0.13	0.06	1.79	0.03
Autres services	0.42	2.86	0.15	0.06	0.89	0.07	0.01	0.71	0.01
Total	10.37	34.70		2.09	15.30		0.40	15.48	

Annexe 4: Procédure de pondération servant à exclure l'influence de la branche d'appartenance / de la taille de l'entreprise

- Plusieurs analyses abordaient l'influence de la taille des entreprises ou de leur branche d'appartenance. Il a donc fallu à chaque fois éliminer l'autre influence.

  Ex.: Dans le secteur financier, 57 % des entreprises interrogées comptaient plus de 250 salariés. Ces entreprises sont donc clairement surreprésentées en comparaison du pourcentage de grandes entreprises dans l'échantillon d'ensemble (16 %). Dans l'hypothèse où une analyse révèlerait que les entreprises du secteur financier investissent beaucoup dans la sécurité informatique, ce constat pourrait découler de la surreprésentation des grandes entreprises dans cette branche.
- Il faut donc utiliser le facteur de pondération w_2, qui évalue les données de telle manière que dans toutes les branches les classes de grandeur soient comparables, et que dans toutes les classes de grandeur les branches soient représentées avec la même fréquence. La formule applicable à w_2 est la suivante:
-

$$w_2 = \frac{n_i / n_{Bi}}{n_{Gi} / N} = \frac{n_i \, N}{n_{Bi} \, n_{Gi}}$$

n_i = nombre d'entreprises de la catégorie i.
n_{Bi} = nombre d'entreprises de la catégorie i.
n_{Gi} = nombre d'entreprises de la taille de la catégorie i.
N = nombre d'entreprises formant l'échantillon.

Calcul de w_2 au moyen du pourcentage des classes de grandeur par branche:

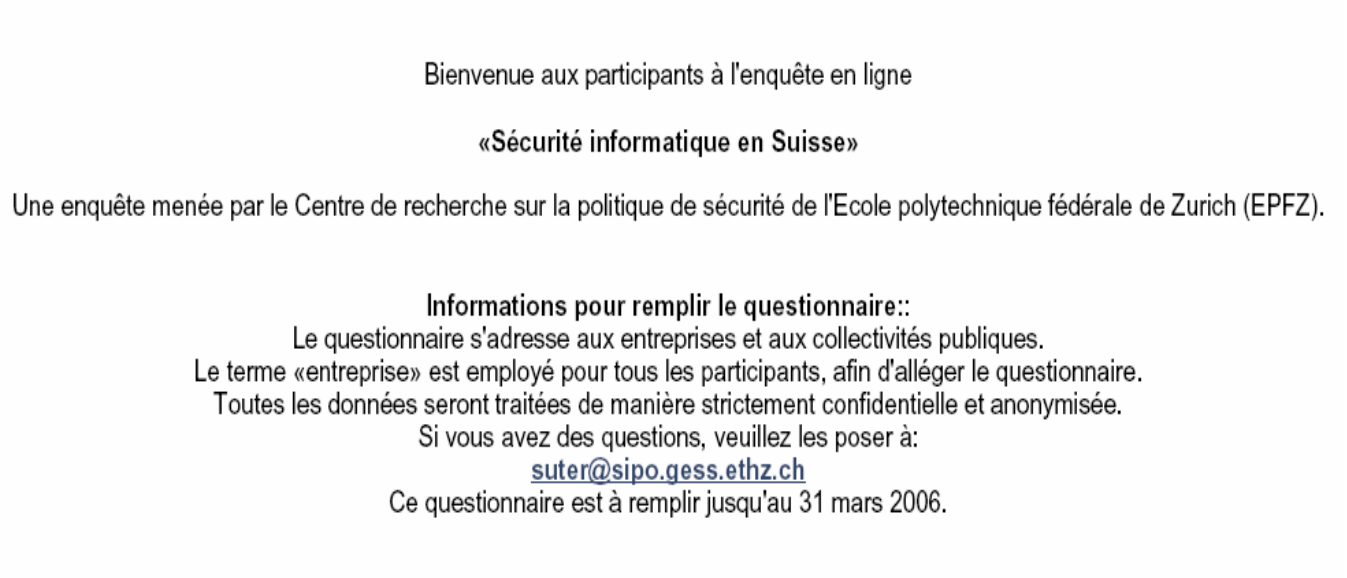
Branche	0-4 (B)	0-4 (M)	Pond	5-9 (B)	5-9 (M)	Pond	10-49 (B)	10-49 (M)	Pond	50-249 (B)	50-249 (M)	Pond	250+ (B)	250+ (M)	Pond
Industrie	9.76	23.57	2.41	4.88	10.89	2.23	31.71	34.82	1.10	26.83	15.19	0.57	26.83	15.52	0.58
Construction	15.22	23.57	1.55	20.65	10.89	0.53	44.57	34.82	0.78	14.13	15.19	1.08	5.43	15.52	2.86
Commerce	30.51	23.57	0.77	10.17	10.89	1.07	44.07	34.82	0.79	5.08	15.19	2.99	10.17	15.52	1.53
Hôtellerie et restauration	10.53	23.57	2.24	10.53	10.89	1.03	63.16	34.82	0.55	10.53	15.19	1.44	5.26	15.52	2.95
Transports et commun.	24.32	23.57	0.97	8.11	10.89	1.34	40.54	34.82	0.86	13.51	15.19	1.12	13.51	15.52	1.15
Activités financières	23.81	23.57	0.99		10.89		14.29	34.82	2.44	4.76	15.19	3.19	57.14	15.52	0.27
Services aux entrepr.	33.96	23.57	0.69	13.21	10.89	0.82	24.53	34.82	1.42	18.87	15.19	0.80	9.43	15.52	1.65
Services informatiques	45.95	23.57	0.51	8.11	10.89	1.34	29.73	34.82	1.17	5.41	15.19	2.81	10.81	15.52	1.44
Administration publique	11.90	23.57	1.98	11.90	10.89	0.92	23.81	34.82	1.46	23.81	15.19	0.64	28.57	15.52	0.54
Enseignement	42.86	23.57	0.55		10.89		42.86	34.82	0.81	7.14	15.19	2.13	7.14	15.52	2.17
Santé	23.64	23.57	1.00	9.09	10.89	1.20	29.09	34.82	1.20	20.00	15.19	0.76	18.18	15.52	0.85
Autres services	34.69	23.57	0.68	14.29	10.89	0.76	32.65	34.82	1.07	10.20	15.19	1.49	8.16	15.52	1.90

(B): Part en pourcentage dans la branche concernée
(M): Part moyenne en pourcentage

Annexe 5: Questionnaire

- L'enquête était organisée en ligne. Tous les participants ont reçu (par poste ou par courriel) une invitation munie d'un mot de passe.
  Ils pouvaient ainsi accéder à la page www.unipark.de/informatiksicherheit.

- L'enquête durait du 15 mars au 13 avril 2006.

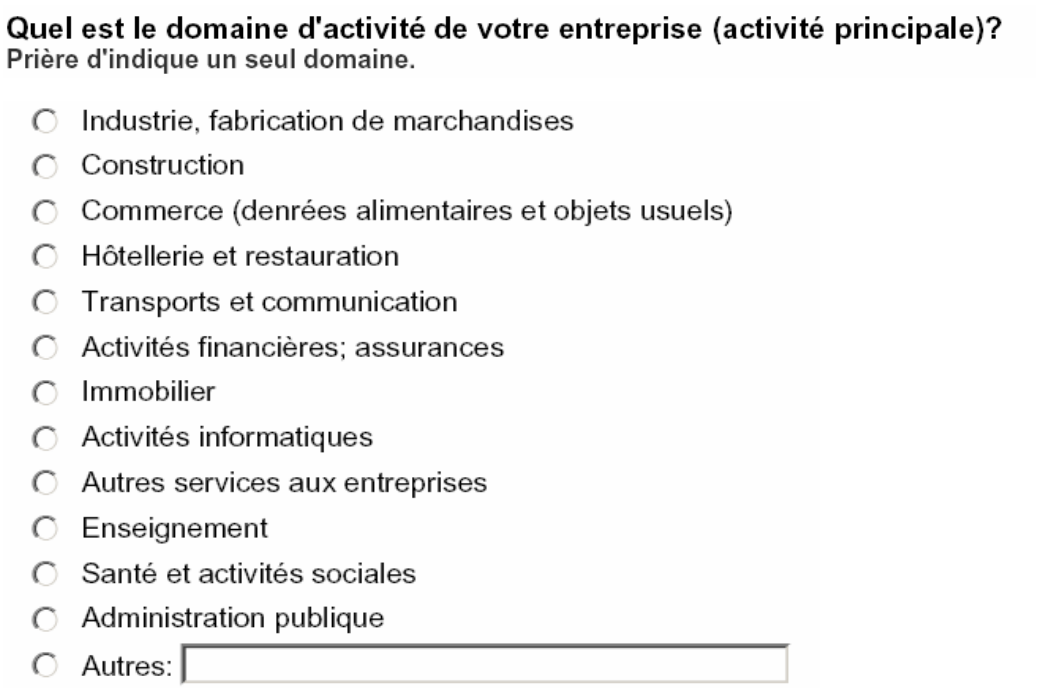


Bienvenue aux participants à l'enquête en ligne

«Sécurité informatique en Suisse»

Une enquête menée par le Centre de recherche sur la politique de sécurité de l'Ecole polytechnique fédérale de Zurich (EPFZ).

Informations pour remplir le questionnaire::
Le questionnaire s'adresse aux entreprises et aux collectivités publiques.
Le terme «entreprise» est employé pour tous les participants, afin d'alléger le questionnaire.
Toutes les données seront traitées de manière strictement confidentielle et anonymisée.
Si vous avez des questions, veuillez les poser à:
suter@sipo.gess.ethz.ch
Ce questionnaire est à remplir jusqu'au 31 mars 2006.



Quel est le domaine d'activité de votre entreprise (activité principale)?
Prière d'indique un seul domaine.

- ○ Industrie, fabrication de marchandises
- ○ Construction
- ○ Commerce (denrées alimentaires et objets usuels)
- ○ Hôtellerie et restauration
- ○ Transports et communication
- ○ Activités financières; assurances
- ○ Immobilier
- ○ Activités informatiques
- ○ Autres services aux entreprises
- ○ Enseignement
- ○ Santé et activités sociales
- ○ Administration publique
- ○ Autres:

Combien de personnes votre entreprise emploie-t-elle?
Inclure les apprentis; convertir le personell à temps partiel en équivalents plein temps; le cas échéant, inclure les collaborateurs actifs à l'étranger.

- ○ 0-4
- ○ 5-9
- ○ 10-49
- ○ 50-249
- ○ plus de 250

Quel a été le chiffre d'affaires de votre entreprise en 2005?
Données en francs suisses.

- ○ Moins de 1 million
- ○ 1 à 4.9 millions
- ○ 5 à 9.9 millions
- ○ 10 à 99 millions
- ○ plus de 100 millions
- ○ Ne sais pas

Quel est le pourcentage d'employés de votre entreprise qui, dans le cadre de leur travail, utilisent les instruments suivants:

	0%	1-20%	21-40%	41-60%	61-80%	81-100%	Ne sais pas
Ordinateur personnel (PC)	○	○	○	○	○	○	○
Ordinateur portatif	○	○	○	○	○	○	○
Assistant numérique personnel (PDA)	○	○	○	○	○	○	○
Téléphone mobile	○	○	○	○	○	○	○
Courriel	○	○	○	○	○	○	○
Internet	○	○	○	○	○	○	○

Vos collaborateurs ont-ils accès de chez eux à votre réseau d'entreprise?

- ○ Oui, et même un accès illimité
- ○ Oui, à certaines conditions
- ○ Non
- ○ Ne sais pas

Quel type de liasion Internet votre entreprise utilise-t-elle?
Plusieurs réponses sont possibles.

- ☐ Modem
- ☐ ISDN
- ☐ DSL (xDSL, ADSL, SDSL etc) < 2Mb/sec
- ☐ Modem câble, ou toute autre liaison à large bande
- ☐ Autres

Votre entreprise utilise-t-elle des réseaux sans fil?

- ○ Oui
- ○ Non
- ○ Ne sais pas

Votre entreprise possède-t-elle son site Internet?

- ○ Oui
- ○ Non
- ○ Ne sais pas

Quelles offres votre site propose-t-il?
Plusierus réponses sont possibles.

- ☐ Informations sur l'entreprise (adresses, but, etc.)
- ☐ Informations sur les produits (publicité)
- ☐ Vente de produits sans procédure de paiment en ligne
- ☐ Vente de produits avec procédure de paiment en ligne
- ☐ Autres

Votre entreprise exploite-t-elle les possibilités souvantes d'Internet?

	Oui	Non	Ne sais pas
Recherche d'informations	○	○	○
Formation et perfectionnement	○	○	○
Forums de discussion	○	○	○
Achat de produits ou de services	○	○	○

Veuilles évaluer l'importance de l'infrastructure informatique pour votre entreprise.

peu importante ○ ○ ○ ○ ○ très importante

Comment la part des investissements réalisés dans l'infrastructure informatique a-t-elle évolué ces cinq dernières années?

baisse	resté stable	croissance	Ne sais pas
○	○	○	○

Avez-vous constaté, pendant l'année 2005, l'une des attaques suivantes contre la sécurité informatique de votre entreprise?

- ☐ Virus, vers, chevaux de Troie
- ☐ Espiogiciels
- ☐ Attaque par saturation (denial of Service, DoS)
- ☐ Intrusion dans le système (hacking)
- ☐ Vol des données
- ☐ Vol d'ordinateurs portables ou d'autre matériel informatique
- ☐ Violation des résaux sans fils
- ☐ Défiguration de site (defacement)
- ☐ Autres
- ☐ Pas constaté une attaque

D'où venaient ces attaques?

- ○ Les attaques venaient de l'extérieur
- ○ Les attaques étaient dues à un collaborateur
- ○ Les attaques ont été aussi bien externes qu'internes

Combien de personnes l'équipe chargée de la sécurité informatique dans votre entreprise comprend-elle?

Prière de convertir en équivalents plein tems les employés à tems partiel.

- ○ personne
- ○ 0 à 1
- ○ 2 à 5
- ○ 6 à 10
- ○ plus de 10

Quelle est la formation du responsable de cette équipe?

- ○ Titre universitaire d'informaticien
- ○ Certificat fédéral de capacité d'informaticien
- ○ Brevet fédéral d'informaticien
- ○ Perfectionnements suivis à titre accessoire dans le secteur de l'informatique
- ○ Autre formation

A combien se sont élevées en 2005, au total, vos dépenses pour la sécurité informatique?

Données en francs suisses. Inclure les frais de personnel et de structure.

- ○ 0 à 5000
- ○ 5001 à 20 000
- ○ 20 001 à 100 000
- ○ plus de 100 000
- ○ Ne sais pas

Selon toute probabilité, votre entreprise dépensera-t-elle davantage ou moins en 2006 pour l sécurité informatique?

- ○ Davantage
- ○ Moins
- ○ Autant
- ○ Ne sais pas

Quel est, dans le domaine de la sécurité informatique, le pourcentage de vos ressources délégué à d'autres entreprises (externalisation)?

0%	1-20%	21-40%	41-60%	61-80%	81-100%	Ne sais pas
○	○	○	○	○	○	○

Dans quelle mesure êtes vous d'accord avec les affirmations suivantes: "Dans le domaine de la sécurité informatique, mon entreprise investit suffisamment de moyens financiers...

	Tout à fait vrai	Plutôt vrai	Cela dépend	Plutôt faux	Tout à fait faux	Ne sais pas
...dans les mécanismes téchniques de protection."	○	○	○	○	○	○
...dans le perfectionnement des responsables informatiques."	○	○	○	○	○	○
...dans le perfectionnement des collaborateurs."	○	○	○	○	○	○

Quels mécanismes de protection utilisez-vous pour garantir la sécurité de vos systèmes informatiques?

Plusieurs réponses possibles.

- ☐ Programmes antivirus
- ☐ Pare-feu
- ☐ Cryptage
- ☐ Programmes anti-espiogiciels
- ☐ Détection d'Intrusion
- ☐ Formation des collaborateurs dans le domaine de la sécurité informatique
- ☐ Biométrie
- ☐ Autres
- ☐ Aucun

Procédez-vous à des analyses régulières de la sécurité informatique?

- ○ Oui, au sein de l'entreprise
- ○ Oui, une entreprise externe s'en charge
- ○ Pas encore, mais il s'agit d'un projet
- ○ Non
- ○ Ne sais pas

Lesquels des concepts suivants utilisez-vous?
Plusieurs réponses sont possibles.

- ☐ Concept de secours informatique (backup management)
- ☐ Politique de sécurité informatique (security policy)
- ☐ Gestion des mises à jour (vulnerability management)
- ☐ Concept de gestion des incidents (incident response)
- ☐ Autres
- ☐ Aucun

Votre entreprise possède-t-elle une assurance couvrant les dommages éventuels causés à votre infrastructure informatique (matériel, logiciels, pertes des données)?

- ○ Oui
- ○ Non
- ○ Ne sais pas

Pour quelles raisons votre entreprise ne possède-t-elle pas d'assurance contre de tels dommages?
Plusieurs réponses sont possibles.

- ☐ Ça ne vaut pas la peine
- ☐ J'ignorais qu'il existe de telles assurances
- ☐ L'argent manque
- ☐ Les offres des assurances laissent à désirer
- ☐ Autrtes

Cherchez-vous (ou votre entreprise) une aide externe en cas de problème lié à la sécurité informatique?

- ○ Oui
- ○ Non
- ○ Ne sais pas

Où?
Plusieurs réponses sont possibles.

- ☐ Fabricants de logiciels
- ☐ Fournisseur de services Internet
- ☐ Collègues/Connaissances dans d'autres entreprises
- ☐ Internet (Web, forums Internet)
- ☐ Autres

Au cas où votre entreprise aurait constaté un accès non autorisé à son système informatique, avez-vous alerté la police?

- ○ Oui
- ○ Non
- ○ Ne sais pas

Pour quelles raisons n'avez-vous pas signalé les incidents à la police?
Plusieurs réponses sont possibles.

- ☐ Ignorance que la police s'intéresse à de tels incidents
- ☐ La police n'offre pas la possibilité d'annoncer de tels incidents
- ☐ Nos propres mesures sont plus efficaces
- ☐ Peur des retombées négatives pour
- ☐ Les incidents semblaient trop peu importants

Utiliseriez-vous les prestations d'un service d'assistance (help desk) spécialisé dans la sécurité informatique?

- ○ Oui, dans tous les cas
- ○ Oui, à condition qu'il soit géré de façon indépendante des fabricants de logiciels
- ○ Non

Un service d'assistance (help desk) pourrait offrir diverses prestations. Lesquelles vous seraient utiles?

	utile	pas utile
Conseils téléphoniques	○	○
Conseils par courriel ou sur la base de tickets	○	○
Conseils personnels sur place	○	○

Les échanges d'expériences et de connaissances entre collègues sont parfois une source utile d'informations. A quel type d'échanges participeriez-vous?

	Participation certaine	Participation probable	Participation peu probable	Participation exclue
Echanges anonymes sur des forums Interne	○	○	○	○
Echanges par des contacts personnels	○	○	○	○
Echanges lors d'ateliers organisés par les fabricants de logiciels concernés	○	○	○	○
Echanges lors d'ateliers organisés par des tiers indépendants	○	○	○	○

D'autres prestations ou documents pourraient vous aider à améliorer votre sécurité informatique. Veuillez indiquer dans quelle mesure les offres suivantes vous seraient utiles.
1 signifie «peu utile» et 5 «très utile».

	1	2	3	4	5
Manuel pourr la procédure de dépôt d'une plainte pénale	○	○	○	○	○
Matériel de base pour la formation ainsi que la sensibilisation des collaborateurs	○	○	○	○	○
Recommandation de pratiques d'excellence (p. ex. ISO 17799)	○	○	○	○	○
Aide pour l'application de pratiques d'excellence (p. ex. ISO 17799)	○	○	○	○	○
Manuel pour la gestion des incidents	○	○	○	○	○

Selon vous, qui serait le plus à même de fournir les prestations indiquées?

- ○ Fabricants de logiciels
- ○ Organisations étatiques
- ○ Associations de branche
- ○ Organisations ad hoc
- ○ Entreprises de conseil

Votre entreprise serait-elle prête à participer financièrement aux coûts de telles prestations?

- ○ Oui, à concurrence de CHF 500.- par an
- ○ Oui, à concurrence de CHF 2000.- par an
- ○ Non
- ○ Ne sais pas

Connaissez-vous MELANI, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération?

- ○ Oui
- ○ Non

Dans quelle mesure MELANI vous est-elle utile pour améliorer la sécurité de vos systèmes informatiques?

peu utile ○ ○ ○ ○ ○ très utile

Les prestations suivantes de MELANI vous sont-elles utiles?

	Oui	Non	Ne sais pas
Mises en garde (Newsticker)	○	○	○
Formulaire d'annonce des incidents	○	○	○
Remarques générales sur les risques et la protection des systèmes d'information	○	○	○
Programmes de démonstration et de formation pour les collaborateurs	○	○	○
Listes de contrôle et instructions pour le personnel	○	○	○
Rapports sur les tendances essentielles et les développements de la sécurité informatique	○	○	○

Auteur

Manuel Suter, lic. phil. I, collaborateur scientifique, Center for Security Studies (CSS), ETH Zurich

Direction de projet

Dr. Myriam Dunn, cheffe du projet New Risks et coordinatrice du Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zurich

Dr. Victor Mauer, directeur adjoint, Center for Security Studies (CSS), ETH Zurich

CSS
An ETH Center

Créé en 1986, **le Bureau de recherche sur la politique de sécurité / Center for Security Studies (CSS)** de l'EPFZ a pour but l'enseignement, la recherche et les prestations de service en matière de politique de sécurité suisse et internationale. Les pôles de recherche portent sur les nouveaux risques, la politique de sécurité européenne et transatlantique, la stratégie et la doctrine, la désintégration et la reconstruction des Etats, ainsi que la politique extérieure et la politique de sécurité de la Suisse. Le Bureau de recherche sur la politique de sécurité gère l'International Relations and Security Network (ISN). Il dispose d'un réseau étendu d'organisations partenaires au niveau national et international et est membre du Centre d'études comparatives et internationales de l'EPFZ et de l'Université de Zurich.