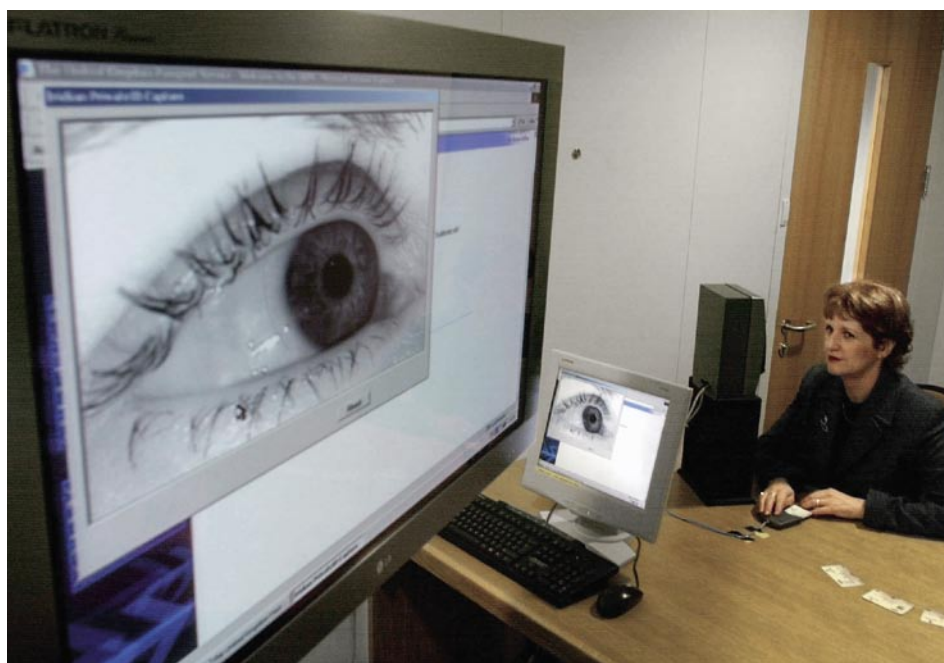


Coopérer pour améliorer la sûreté de l'information dans les entreprises

La plupart des entreprises ne pourraient plus concevoir leur quotidien sans les technologies de l'information et de la communication (TIC), qui leur permettent de travailler en réseau de façon coordonnée et forment la base d'importants processus. Pour nombre d'entre elles, une panne ou un arrêt du système d'information aurait des conséquences graves. Protéger les TIC ainsi que les données transmises et stockées constitue, toutefois, une vraie gageure. Comme les menaces techniques évoluent à toute vitesse, il faut sans cesse prendre de nouvelles mesures de prévention.

L'échange d'expériences aiderait beaucoup d'entreprises à maintenir leurs connaissances à jour.

L'État peut participer activement à une telle coopération et contribuer ainsi à améliorer la sécurité.



La sûreté de l'information ne peut être garantie par les seuls moyens techniques, tels la biométrie (en illustration). Comme de nombreuses entreprises se heurtent aux limites de leurs capacités en matière de gestion des risques et des incidents, il est important qu'elles se soutiennent mutuellement.

Photo: Keystone

Un défi technique et organisationnel

Garantir la sûreté de l'information représente un énorme défi pour les entreprises. Il s'agit de corriger à temps les failles de sécurité des systèmes employés et de réagir à des attaques aux méthodes toujours nouvelles en introduisant des programmes de protection appropriés. Cela commence par des mesures d'ordre technique. De nos jours, presque toutes les entreprises utilisent des logiciels antivirus et des pare-feu. Nombre d'entre elles appliquent, en outre, des techniques de cryptage et des programmes de détection des attaques. Quelques-unes recourent même à des méthodes biométriques pour protéger leurs ordinateurs des visites indiscretes.



Manuel Suter
Center for Security
Studies, EPF Zurich

Avec le temps, il est, cependant, devenu de plus en plus évident que les problèmes de sécurité ne pouvaient être maîtrisés par les seuls moyens techniques. Malgré des investissements substantiels dans ce domaine, attaques et incidents continuent de perturber les systèmes d'information de nombreuses entreprises. Les mesures techniques s'avèrent inefficaces si elles ne sont pas appliquées rigoureusement et correctement. C'est pourquoi la sûreté de l'information est un défi non seulement technologique, mais également organisationnel. La formation des collaborateurs, la gestion de la sécurisation des données, les plans d'urgence et de crise ainsi que les examens réguliers de la sécurité sont aujourd'hui des éléments tout aussi importants que les dispositifs de protection mentionnés plus haut.

Besoin d'experts

La sûreté de l'information est une tâche complète et exigeante, parce qu'il faut mettre en œuvre des mesures aussi bien techniques qu'organisationnelles. Elle réclame des efforts constants, car les menaces et les risques

évoluent sans cesse, de même que les ripostes possibles. En outre, il est parfois difficile pour les entreprises de juger si leur protection est suffisante. Le calcul coût/bénéfice n'est guère possible, faute de statistiques fiables quant à la fréquence des incidents et à l'ampleur des dommages consécutifs.

Pour toutes ces raisons, les entreprises se heurtent souvent aux limites de leurs capacités, en ce qui concerne non seulement le traitement des incidents, mais aussi la gestion des risques. Nombre d'entre elles dépendent du savoir des experts. Or, les conseils et l'assistance externes sont trop coûteux pour beaucoup de petites et moyennes entreprises (PME). Il peut en résulter des failles de sécurité propices à des attaques, qui ne causeront pas seulement des problèmes à l'entreprise concernée, mais aussi à d'autres. En effet, les pirates informatiques peuvent relier entre eux des ordinateurs mal protégés, créant ainsi des «réseaux de zombies» dont ils utilisent la puissance de calcul pour des attaques à la fois ciblées et sophistiquées contre des objectifs mieux protégés. Aussi est-il important que les entreprises s'entraident pour relever les défis liés à la gestion des incidents et des risques. On débattrait ci-dessous de quelques-unes des voies possibles.

Soutien en cas d'incident: les équipes d'intervention en cas d'urgence informatique

En 1988 déjà, les exploitants de l'Arpanet, réseau considéré comme le précurseur de l'actuel Internet, ont dû affronter des problèmes de sécurité. Un étudiant, Robert Morris, avait programmé à l'époque le premier «ver» informatique, qui paralysa environ 10% des quelque 60 000 ordinateurs connectés. Au plus tard après cet incident, il devint évident que la sûreté de l'information au sein des réseaux posait des exigences entièrement nouvelles, auxquelles seule une action coordonnée pouvait répondre.

C'est alors que fut fondée la première *équipe d'intervention en cas d'urgence informatique* (en anglais «*Computer Emergency Response Team*», Cert) à l'université Carnegie Mellon de Pittsburgh. L'idée était de constituer un réseau d'experts pour maîtriser rapidement et efficacement de tels incidents. Ce modèle s'est avéré très performant et a largement contribué à répondre aux attaques contre les réseaux informatiques. Mais depuis lors, Internet a crû dans des proportions spectaculaires. Aujourd'hui, un seul Cert ne suffirait jamais à gérer tous les incidents et attaques. C'est pourquoi nombre d'États et de grandes entreprises ont mis sur pied leurs propres Cert. Ces différents groupes d'ex-

perts sont responsables de la sûreté informatique de leurs mandants respectifs et travaillent en étroite collaboration. L'association internationale *Forum of Incident Response and Security Teams (First)* représente actuellement plus de 190 Cert dans 140 pays.

Le rôle des Cert est souvent comparé à celui des pompiers, qui interviennent en cas d'accident, mais sont aussi engagés dans la prévention. Grâce à leur expertise technique, ces organismes sont en mesure d'émettre très tôt des alertes concernant de nouvelles attaques et d'aider les entreprises à verrouiller leurs points faibles. Malgré ces activités préventives, il ne faut pas oublier que les Cert sont d'abord responsables de la sécurité des réseaux d'ordinateurs et qu'ils ne peuvent se soucier de la gestion des risques de telle ou telle firme. C'est pourquoi d'autres mesures sont nécessaires pour aider les entreprises dans cette tâche.

Améliorer la gestion des risques par l'échange d'informations

Les entreprises ne peuvent gérer judicieusement les risques que si elles connaissent les menaces et les ripostes possibles. L'échange d'expériences est un moyen très prometteur d'acquérir ces connaissances. Quand des entreprises se fournissent mutuellement des informations sur les attaques qu'elles ont subies et sur les ripostes possibles, elles acquièrent de façon simple un savoir-faire précieux et peuvent adopter des mesures de protection ciblées.

Il existe déjà des collaborations informelles entre entreprises dans ce domaine. Une étude sur la sûreté de l'information dans les entreprises suisses a révélé que 40% des responsables de sociétés ayant connu un incident informatique en ont discuté avec des collègues d'une autre entreprise. Presque 25% d'entre eux sont allés de surcroît chercher des informations sur Internet, ce qui représente également une forme d'échange d'informations interentreprises (voir *graphique 1*).

Le partage d'expériences se pratique donc, bien qu'il porte souvent sur des données très sensibles pour les entreprises. Pour des raisons de prestige mais aussi de sécurité, ces dernières ont en effet intérêt à ce que l'on n'apprenne en aucun cas où se situent leurs points faibles et de quels incidents elles ont été victimes; l'échange d'informations ne peut donc avoir lieu que dans un climat de confiance totale. Sur ce point, les réseaux informels de responsables d'entreprises sont d'une grande valeur, mais ils dépendent fortement des personnes et sont donc relativement éphémères en raison des fluctuations

Encadré 1

Qu'est-ce que la sûreté de l'information?

La sûreté de l'information a pour but d'empêcher la modification ou l'obtention non autorisées d'informations ou de données. La sécurité informatique, celle des réseaux et celle des données en constituent des aspects partiels importants.

Dans les entreprises, la sûreté de l'information est menacée d'une part par les attaques, c'est-à-dire les accès ou tentatives d'accès non autorisés à un système. Les informations peuvent également être modifiées ou détruites par des incidents, à savoir de fausses manipulations involontaires, sans intention malveillante, ou des pannes techniques. Selon les risques d'attaque ou d'incident menaçant la sûreté de l'information, on prend des mesures aussi bien techniques (axées sur les systèmes informatiques) qu'organisationnelles (axées sur les utilisateurs).

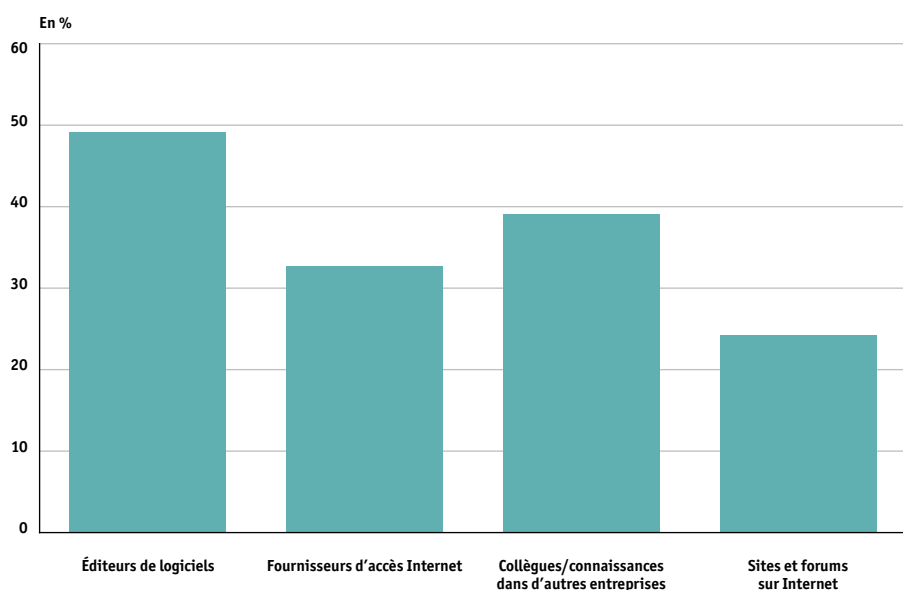
Encadré 2

Information Sharing and Analysis Centers (Isac)

Les Isac américains sont les organisations les plus connues d'échange d'informations interentreprises en matière de sûreté de l'information. Ils ont été lancés par le gouvernement pour mieux protéger les infrastructures sensibles et rassemblent les principales firmes de chacun des secteurs économiques cruciaux. L'organisation interne est laissée au soin des entreprises, raison pour laquelle les quinze Isac officiels existants ont une structure et une taille différentes. Les autorités responsables des secteurs respectifs collaborent étroitement avec les Isac afin de promouvoir ainsi l'échange d'informations interentreprises.

Graphique 1

Où les entreprises vont-elles chercher de l'aide après des incidents ayant affecté leur sûreté informatique?



Source: Suter (2006) / La Vie économique

de personnel. Pour améliorer durablement la sûreté de l'information, il faut instaurer la confiance entre entreprises sur une base solide. Cela nécessite une coopération bien structurée et coordonnée, en d'autres termes une organisation qui offre à ses membres une plate-forme pour leurs échanges.

Les difficultés de la coopération

Il n'est pas simple de mettre sur pied une telle organisation pour répondre aux exigences mentionnées. Les entreprises sont souvent en concurrence directe ou indirecte, ce qui implique des risques pour toutes celles qui participent aux échanges d'informations. Or, il est impossible d'évaluer à l'avance si la coopération fonctionnera effectivement de telle sorte que toutes les informations transmises resteront confidentielles. Le problème est qu'une confiance indépendante des personnes ne peut naître qu'au terme d'une longue collaboration, cette dernière réclamant à son tour de la confiance. Un problème analogue se pose quant à l'utilité des échanges: les entreprises ne sont disposées à y participer que si l'intérêt des informations obtenues dépasse le coût des efforts consentis; elles ont donc tendance à n'adhérer à de telles organisations que quand celles-ci ont déjà démontré leur utilité.

Dans les sciences sociales et économiques, ces situations sont décrites comme des problèmes de coopération et de coordination. Elles expliquent pourquoi la collaboration ne s'instaure pas automatiquement, même si elle profite à tous les participants; elles ne

peuvent souvent être surmontées qu'avec l'aide d'un coordinateur externe.

Partenariats public-privé

Dans beaucoup de pays, ce rôle de coordinateur est assumé par l'État. La sûreté de l'information dans les entreprises est promue avant tout par des partenariats public-privé (PPP). Dans de nombreux États, des PPP ont été conclus avec les exploitants d'infrastructures sensibles – autrement dit des entreprises dont les prestations ont une importance cruciale pour l'économie et la société¹. Ils permettent aux entreprises impliquées d'avoir un accès direct aux autorités, par exemple à celles chargées de l'exécution des peines. L'État offre, en outre, à ses partenaires privés des informations dont ils ne disposeraient pas autrement, comme des rapports sur les activités d'organisations criminelles internationales. Ce type de coopération favorise directement la sûreté de l'information de firmes importantes.

De son côté, l'État demande aux entreprises partenaires de rendre accessibles aux autres membres du PPP leurs expériences et connaissances en matière de sûreté de l'information. Une telle coopération instaure un climat de confiance entre les firmes, ce qui désamorce les problèmes de collaboration et facilite l'échange d'informations. Ainsi, l'État contribue indirectement à améliorer la sécurité informatique des entreprises.

Les modèles les plus connus de PPP dédiés à l'échange d'informations sont les «*Information Sharing and Analysis Centers*» (Isac) aux États-Unis (voir encadré 2). En Suisse, la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information* (Melani) offre une plate-forme d'échanges aux entreprises dont les prestations ont une importance cruciale pour l'économie et la société.

Soutien aux PME

Une coopération aussi intense entre l'État et le secteur privé se limite forcément à quelques entreprises triées sur le volet, puisqu'il est impossible d'offrir à toutes des informations exclusives et un accès direct aux autorités chargées de l'exécution des peines. La sûreté de l'information des PME doit donc être encouragée par d'autres moyens.

Il importe en premier lieu de sensibiliser les PME aux risques affectant la sûreté de l'information et de les renseigner sur les possibilités de protection. Les entreprises pourraient souvent augmenter, dans d'importantes proportions, la sécurité de leurs données en mettant simplement en œuvre les principales mesures de protection. En Suisse, l'as-

1 Voir l'article de Ruedi Rytz, p. 57ss de ce numéro.

Bibliographie

- Abele-Wigert Isabelle et Dunn Myriam, *International CIIP Handbook 2006, vol. I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, Zurich, 2006.
- Anderson Ross et Moore Tyler, «The Economics of Information Security», *Science*, vol. 314, 2006, p. 610–623.
- Grady Mark F. et Parisi Francesco (éd.), *The Law and Economics of Cybersecurity*, Cambridge, 2006, Cambridge University Press.
- Dunn Myriam et Mauer Victor (éd.), *International CIIP Handbook 2006, vol. II: Analyzing Issues, Challenges, and Prospects*, Center for Security Studies, Zurich, 2006.
- Suter Manuel, *Informationssicherheit in Schweizer Unternehmen. Eine Umfragestudie über Bedrohungen, Risikomanagement und Kooperationsformen*, Center for Security Studies, Zurich, 2006.
- 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 I/2007*. Internet: www.melani.admin.ch, «Documentation», «Rapports sur la situation».

sociation InfoSurance se bat pour que les PME bénéficient d'une meilleure information².

Comme il le fait dans les PPP conclus avec de grandes entreprises, l'État peut également essayer de promouvoir l'échange d'informations entre PME en offrant une plate-forme ad hoc et en renforçant la confiance interentreprises par sa médiation. Le gouvernement britannique a donné l'exemple d'une telle initiative avec son programme portant sur la création de services d'alerte, de conseil et de notification («Warning, Advice and Reporting Points», Warp). Ce programme encourage l'échange d'informations entre entreprises en mettant un logiciel spécifique à leur disposition ainsi que du matériel publicitaire. Il transmet, en outre, les expériences des Warp existants aux groupes intéressés qui voudraient en créer de nouveaux. S'adressant surtout aux PME, il prévoit de faciliter le partage d'informations entre des entreprises de même taille et du même secteur économique (ou de la même région). C'est pourquoi un Warp compte rarement plus de cent entreprises. Comme le programme est soutenu par le gouvernement, elles

peuvent tabler sur la continuité et la fiabilité des échanges.

Aide à l'auto-assistance

Les PPP, les campagnes d'information et les programmes d'échange se fondent tous sur le principe de l'aide à l'auto-assistance. En fournissant des informations importantes, en s'engageant dans des associations qui visent à sensibiliser les entreprises ou en donnant l'impulsion à des échanges d'expériences et de connaissances entre ces dernières, l'État peut fortement contribuer à améliorer la sûreté de l'information. Ce n'est que par le regroupement des forces disponibles et le partage d'expériences et de connaissances que l'on parviendra à maîtriser les divers défis en mutation constante qui guettent la sûreté de l'information. ■

² Voir l'article de Carlos Rieder, p. 60ss de ce numéro.

Financing for Climate Innovative Solutions and New Markets

11–12 September 2008, Swiss Re Centre for Global Dialogue Rüschlikon, Switzerland



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs FDEA
State Secretariat for Economic Affairs SECO



Financial markets are expected to play a crucial role in promoting and implementing climate change mitigation and adaptation strategies and measures. Suitable financial instruments can foster commercially viable and high impact climate-related investments, provide necessary funding for climate protection in emerging and developing countries, and help efficiently mitigate the associated risks.

High-level speakers including

- Jacques Aigrain (CEO, Swiss Re),
- Doris Leuthard (Federal Councillor, Head Federal Department of Economic Affairs, Switzerland),
- Lars Thunell (CEO & EVP, International Finance Corporation)

and prominent experts, will:

- provide a comprehensive overview of the market; and specific financial innovations,
- explore opportunities and challenges for viable private sector investments and public-private partnerships,
- identify success factors for sustainable climate-related investments based on best practice examples.

during plenary and working sessions on:

- climate-related funds,
- project and corporate finance,
- carbon market and weather risk transfer solutions from the capital markets,
- identification of specific follow-on investment and partnership opportunities.

Registration and further information:

<http://www.sustainability-zurich.org/financing-for-climate>