PAR LUC-FRANÇOIS SALVADOR

président-directeur général du groupe Sogeti

La **sécurité**, un défi à **relever**

Les systèmes d'information sont soumis à des menaces importantes susceptibles d'être à l'origine de dégâts considérables pour l'entreprise, voire de désastres. Cependant, la sécurité cesse d'être une préoccupation lorsqu'on la traite de manière professionnelle. L'entreprise peut alors parvenir à un niveau de risque maîtrisé et acceptable, cohérent avec ses enjeux. La sécurité ne freine plus le développement de l'entreprise et permet l'introduction sans risque de technologies prometteuses.

REPÈRES

Les attaques informatiques contre l'économie numérique s'accroissent très fortement depuis quelques années : blocage ou défiguration de sites Internet, appropriation et parfois mise en ligne d'identifiants ou de données personnelles, intrusion dans les systèmes d'information, interception de communications électroniques, piégeage de dispositifs numériques (logiciels ou matériels) et maintenant accès malveillant à des systèmes numériques de contrôle industriel.

L'accès malveillant aux systèmes de contrôle industriel pourrait provoquer des catastrophes

Il n'est plus de conflit entre États ou entre communautés, de mouvement protestataire qui ne se double d'attaques des systèmes d'information, parfois très sophistiquées, par des « hackers » ou des « hacktivistes » de plus en plus compétents. Si de telles attaques étaient généralement bénignes ou épisodiques il y a encore quelques années, elles atteignent désormais souvent un haut niveau de professionnalisme et visent des cibles qui pouvaient s'estimer bien protégées (banques, sociétés de sécurité informatique, autorités de certification numérique, systèmes gouvernementaux ou couverts par le secret de la défense nationale, etc.).

Pertes et catastrophes

Les conséquences de cette insécurité sur l'économie sont de plus en plus lourdes. Par ordre de gravité croissante :
– les atteintes au bon fonctionnement des sites et des systèmes se traduisent en pertes de chiffres d'affaires de plusieurs jours ;
– les interceptions de communications électroniques ainsi que les intrusions dans les systèmes d'information donnent lieu à des vols massifs d'informations sensibles de l'entreprise ;
– les appropriations de données sensibles ou personnelles entraînent de graves atteintes à la réputation de l'entreprise ainsi qu'à celle de ses dirigeants ;
– l'accès malveillant aux systèmes numériques de contrôle industriel pourrait provoquer des catastrophes majeures. D'ores et déjà, des vulnérabilités informatiques ont été découvertes et publiées sur Internet pour nombre de systèmes de contrôle existants. Des cas – encore ponctuels, fort heureusement – d'attaques de tels systèmes ont été observés.

Des régimes juridiques particuliers

Outre ces menaces qui relèvent de la cybercriminalité, certains risques pour la sécurité de l'information dérivent de régimes juridiques nationaux. En particulier, la législation américaine introduite par le « Patriot Act » permet aux autorités américaines et aux services de ce pays d'exiger de toute entreprise soumise à la juridiction américaine l'accès à ses données. Et cela, que celles-ci soient localisées sur le territoire américain ou non, sans égard pour les règles issues du droit local ou du droit européen, pourtant très protecteur, mais qui se révèle inopérant en l'espèce. Ainsi, confier ses données – ou celles de ses clients – à un prestataire dont la maison mère est localisée aux États-Unis les expose à un risque de divulgation, quel que soit le cadre légal ou contractuel de la prestation correspondante.

Atteinte à la vie personnelle

Demain, l'Internet des objets placera à la portée des pirates du Net la plupart des objets de notre vie personnelle (quand ce n'est pas déjà le cas – nos téléphones mobiles, par exemple) : équipements de la maison, véhicules, implants et autres dispositifs médicaux, bientôt nos montres et nos clés, pour ne citer que quelques-uns de ceux que l'on peut aisément identifier aujourd'hui.

Éviter un désastre pour l'entreprise visée

Au vu des dernières vagues d'attaques connues, de plus en plus d'acteurs économiques prennent conscience de l'importance de sécuriser leur activité.

Certains, les banques par exemple, en sont convaincus de longue date et veillent à maintenir leurs défenses à bon niveau face à la menace dont la sophistication augmente chaque semaine.

D'autres, qui s'étaient jusqu'à présent contentés de mesures de sécurité élémentaires (antivirus, *firewall*), améliorent leur vigilance quotidienne (hygiène informatique) et mettent en place des solutions élaborées de protection ou de défense.

Bien que les attaques touchent toutes sortes d'entreprises et d'administrations, il est possible d'accroître considérablement le niveau de sa sécurité en menant une analyse de risques, en mettant en place et en conduisant un plan de renforcement de la sécurité et en gérant attentivement sa sécurité au quotidien. L'efficacité de ces actions se vérifie par des audits et des tests de pénétration assurés par des prestataires. Une entreprise qui aura mené une telle démarche sera protégée face aux attaques simples, qui constituent 99 % des agressions observées, et limitera considérablement les dommages qu'engendrerait une attaque sophistiquée. En outre, elle facilitera les poursuites judiciaires des agresseurs.

Pas d'impasse sur la sécurité

Plusieurs technologies novatrices ne demandent qu'à se déployer en masse dans les entreprises car elles répondent à de forts besoins exprimés par les cadres ou les métiers de l'entreprise. Ainsi en est-il de l'accès à distance au système d'information, du *cloud computing* (externalisation du stockage et du traitement de l'information sur des serveurs virtuels non localisés à l'avance), de l'utilisation à des fins professionnelles d'équipements informatiques personnels *(bring your own device)*, du raccordement généralisé des équipements de production au système d'information de l'entreprise. Cependant, les risques pour la sécurité de l'entreprise de ces démarches sont parfois tels que le déploiement ne peut s'organiser que dans le cadre d'une démarche de sécurité bien conduite. Certaines de ces nouvelles technologies étant très largement, voire exclusivement, d'origine nord-américaine (terminaux mobiles et leurs logiciels, *cloud computing*), peu d'opérateurs français ou européens en maîtrisent la sécurité, ce qui en ralentit encore la diffusion dans les entreprises.

L'analyse de risques protège contre la majorité des agressions observées

La démarche de sécurisation

La sécurité d'un système d'information repose avant tout sur de bonnes pratiques d'administration des systèmes (« l'hygiène informatique »). Dès lors que le système est correctement administré, une démarche de sécurisation construite peut se mettre en place. Il s'agit tout d'abord de mener une analyse de risques et d'identifier les informations, les applications et les infrastructures réellement sensibles sur le réseau de l'entreprise. Une évaluation du niveau de sécurité existant et un plan de renforcement de la sécurité peuvent alors être établis.

Sur cette base, des projets de sécurisation sont alors conduits (politique de sécurité des systèmes d'information, sécurisation des mots de passe et authentification forte, gestion automatisée des mises à jour des logiciels, formation des administrateurs système et sensibilisation du personnel, identification et contrôle d'accès renforcés, etc.).

Un service de détection des attaques en temps réel et d'administration de la sécurité peut être mis en place, éventuellement avec l'aide d'un prestataire qualifié. À l'issue, et régulièrement par la suite, des audits et des tests de pénétration fournissent une évaluation de l'efficacité de la démarche. Celle-ci peut être structurée et rendue pérenne *via* une certification ISO 27001 de l'entreprise.

L'évolution du marché de la sécurité

Le marché de la sécurité informatique est estimé à 60 milliards de dollars au niveau mondial. Il s'accroît rapidement et devrait représenter en 2013 environ 14 % du marché de l'informatique. Pour le seul segment du conseil et des prestations de service, il s'accroît de 11 % par an. Bien que ces chiffres soient importants, ils restent largement inférieurs aux dommages économiques entraînés par les attaques informatiques. Aujourd'hui très éclaté, le marché de la sécurité informatique se structure du côté de la demande (prise de conscience de l'ampleur des besoins) comme du côté de l'offre (mise en place de compétences globales, industrialisation de la démarche).

La demande se structure et s'accroît

Du côté de la demande, un nombre croissant de sociétés entreprennent une démarche systématique de sécurité telle que résumée ci-dessus et affectent à cet objectif les priorités et les ressources nécessaires. Elles dépassent le stade des achats ou des prestations de sécurité ponctuelles, veillent à leur hygiène informatique et organisent de manière professionnelle la montée en puissance de leur sécurité (évaluation de l'existant et analyse de risques, mise au point d'un plan de renforcement, conduite de projets de sécurisation, vérification par des audits et tests, mise en place d'une démarche permanente de renforcement).

Aujourd'hui, de plus en plus de sociétés prennent du reste conscience de la nécessité de se faire assister par un « prestataire global de sécurité informatique », capable de les aider à analyser leur situation, de construire leur sécurité, de surveiller leurs réseaux et de s'assurer du maintien à jour permanent de la démarche.

Le déploiement de technologies novatrices exige une démarche de sécurité bien conduite

L'offre se professionnalise

Du côté de l'offre, quelques sociétés françaises, nécessairement de taille importante, commencent à déployer l'ensemble des compétences nécessaires pour pouvoir offrir à leurs clients une offre cohérente et globale de sécurité.

Elles mettent en place des prestations forfaitaires, telles que la surveillance permanente des réseaux *via* des *security operation cen-*

L'impact économique des cyberattaques

En 2011, un rapport fourni au Premier ministre britannique évaluait l'impact de la cybercriminalité sur l'économie nationale à au moins 27 milliards de livres, supportés pour les trois quarts par les entreprises. Ces coûts sont causés, par ordre décroissant d'importance, par la perte de propriété intellectuelle, l'espionnage économique, les extorsions de fonds, le vol en ligne et la perte de données des clients.
Selon la société américaine de sécurité Symantec, le préjudice total causé par la cybercriminalité dans le monde s'élèverait à 388 milliards de dollars, composés pour 30 % du préjudice direct dû aux attaques et pour 70 % du temps perdu par les victimes. En France, ce préjudice total s'élèverait à plus de 1,7 milliard d'euros et concernerait près de 10 millions de victimes chaque année.

Quelques attaques récentes

En 2010, un code informatique malveillant particulièrement sophistiqué visait spécifiquement les installations nucléaires iraniennes. Il aurait provoqué la casse de nombreuses centrifugeuses.
En mars 2011, les ministères économiques et financiers annonçaient l'existence d'une vaste intrusion informatique ayant occasionné la fuite de nombreux documents sur l'action de la France dans l'économie internationale, notamment lors de sa présidence des G7 et G20.
En mars 2011, le fournisseur américain de solutions de sécurité informatique RSA signalait avoir subi une agression informatique très sophistiquée. Les informations confidentielles ainsi obtenues étaient par la suite utilisées par les attaquants pour voler des informations sensibles dans les systèmes d'information d'entreprises travaillant dans le domaine de la défense.
Au printemps 2011, des *hackers* annonçaient avoir pénétré des systèmes d'information du groupe Sony et y avoir dérobé les informations personnelles de plus de cent millions de clients des services en ligne de l'entreprise, qui ont dû être interrompus pendant plusieurs semaines.

ters, ouverts 24 heures sur 24, qui mutualisent les prestations pour plusieurs clients et permettent à chacun de ceux-ci de bénéficier de prestations individualisées de très haut niveau avec des coûts partagés. Elles doivent être capables d'intégrer les solutions et les équipements de sécurité fournis par les PME françaises et, de ce fait, de fédérer le tissu industriel correspondant. Elles s'inscrivent dans un partenariat de confiance avec l'État qui leur permet de disposer des informations les plus récentes sur la menace et les bonnes pratiques et de garantir leur sérieux et leur professionnalisme à leurs clients.

Un rapport étroit avec l'État

Compte tenu des enjeux régaliens et du caractère stratégique de la sécurité des systèmes d'information, qui concerne les organismes les plus sensibles de l'État au même titre que les acteurs économiques, l'État et les entreprises compétentes et de confiance doivent plus que jamais travailler ensemble pour faire face aux menaces qui pèsent sur l'économie numérique.
Au sein de l'État, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en 2009 et a été désignée autorité nationale de sécurité puis, plus récemment, de défense des systèmes d'information. Elle définit la politique et coordonne les actions de l'État dans le domaine et assure, en cas d'attaque informatique majeure visant les systèmes d'information nationaux essentiels, la défense numérique de la nation en liaison avec les ministères et les opérateurs directement concernés. Il est remarquable de constater que, en ces temps de restrictions budgétaires, l'État a su investir fortement et judicieusement dans un sujet majeur pour l'économie nationale.

Partenariat public-privé

Comme il l'a annoncé en 2011 dans la stratégie nationale de défense et de sécurité des systèmes d'information, l'État a entrepris de mettre sur pied un partenariat public-privé avec des opérateurs de confiance afin que la protection informatique des infrastructures essentielles au bon fonctionnement de la Nation soit mieux assurée.
Piloté par l'ANSSI, ce partenariat doit en particulier permettre de diffuser les bonnes pratiques de sécurité et de partager l'analyse de la menace. Il implique au premier chef des industriels et prestataires de service dans le domaine de la sécurité. ■

L'exemple de Sogeti

**Sogeti, filiale à 100 % du groupe Capgemini, est dédiée aux services informatiques de proximité pour les entreprises.
Avec 20 000 employés, dont près de 10 000 en France, elle est présente dans une quinzaine de pays dans le monde. Sogeti a mis en place une offre complète de prestations destinée à répondre à l'ensemble des besoins en sécurité de ses clients. Cette offre va du conseil et de l'analyse de risques jusqu'à la mise en place de solutions de sécurité ou à la gestion permanente de la sécurité numérique de l'entreprise. Elle s'étend jusqu'à la maîtrise d'œuvre de la sécurité et de la défense des systèmes d'information de ses clients.**

La lutte informatique offensive

**Le Livre blanc sur la défense et la sécurité nationale, élaboré par le gouvernement en 2008, annonce que la France se dote d'une capacité de neutralisation par voie informatique des centres d'opérations adverses. Les forces armées se préparent à conduire de telles actions et, à cette fin, mettent en place des cellules spécialisées et se dotent d'équipements et d'outils adaptés. Adapté à un contexte militaire ce cadre d'emploi se doit de respecter le principe de riposte proportionnelle à l'attaque, visant en priorité les moyens opérationnels de l'adversaire.
Les États-Unis, de leur côté, ont mis en place au niveau stratégique un *cyber command*, opérationnel depuis 2010 et placé sous l'autorité d'un officier général également directeur de la National Security Agency. Le *cyber command* est chargé de préparer et de conduire les opérations américaines de lutte informatique offensive.
Pour mémoire, en dehors du cadre militaire, les actions informatiques à visée offensive sont naturellement interdites par la loi.**

L'État a su investir fortement et judicieusement dans un sujet majeur pour l'économie nationale