Plus que des technologies

Si je vous demandais comment sécuriser les données enregistrées dans votre microordinateur, vous me parleriez sans doute de logiciels antivirus, de pare-feu ou de procédures d'accès. Il existe également d'autres moyens…

Par Gilles Drouin

En effet, ces éléments, bien qu'essentiels, ne représentent qu'une petite partie des procédés ou des outils qui protègent vos données. Selon l'Institut pour la sécurité de l'information du Québec (ISIQ), la sécurité de l'information englobe l'ensemble des systèmes d'exploitation, des réseaux de télécommunication, des logiciels, des applications, des documents ou des données, de même que la sécurité physique des lieux et des équipements.

Un tel spectre implique une approche globale qui comprend aussi bien une conception plus robuste des logiciels et de la quincaillerie informatique que l'aménagement des bureaux et l'acquisition de bonnes habitudes assurant la sécurité. « Ces mesures peuvent être aussi simples qu'une bonne ventilation pour éviter la surchauffe de l'équipement », indique l'ingénieur François Coallier, directeur du Département de génie logiciel et des technologies de l'information de l'École de technologie supérieure (ETS).

François Coallier, ing.

CONFIDENTIALITÉ, INTÉGRITÉ ET DISPONIBILITÉ

La sécurité de l'information compte trois grandes dimensions : la confidentialité, l'intégrité et la disponibilité. De façon

générale, la première consiste à contrôler l'accès aux données afin qu'elles ne soient lues que par des personnes autorisées et dans un contexte d'utilisation bien défini. La deuxième renvoie à la nécessité de s'assurer que les données ne sont pas modifiées subrepticement. Enfin, il faut en même temps veiller à ce que l'information soit toujours accessible à l'utilisateur autorisé, quelles que soient les circonstances.

L'informaticien Luc Poulin, conseiller senior en sécurité à l'ISIQ, prépare un doctorat en informatique. Il a décortiqué les domaines de connaissances qui entrent en jeu en matière de gestion de la sécurité de l'information. De façon globale, cette gestion relève à la fois de la gouvernance de l'entreprise, de la conception et de l'entretien des infrastructures, du développement et de l'évolution des applications et des systèmes, ainsi que des activités de vérification et de contrôle visant à assurer la conformité.

Luc Poulin

Ces quatre domaines gravitent autour d'un point central qui est constitué des informations que l'entreprise ou l'organisation estime crucial de sécuriser. « Il est essentiel de tenir compte des quatre domaines pour protéger les données critiques et les quatre doivent être mis en application de la meilleure façon possible », précise Luc Poulin.

LA GOUVERNANCE

Contrairement à ce que l'on pense bien souvent, la sécurité est d'abord une affaire de gouvernance, de gestion, avant d'en être une de technologie. « La sécurité de l'information est un élément de la gestion des risques au sein d'une entreprise ou d'une organisation », mentionne François Coallier. Les risques sont nombreux : vol, destruction ou manipulation des données, informations inaccessibles ou corrompues, utilisation impossible des équipements informatiques à la suite d'un désastre, et j'en passe.

« La sécurité doit d'abord répondre aux objectifs d'affaires d'une entreprise », souligne Richard Neault, conseiller senior en sécurité à l'ISIQ. « On n'improvise pas le déploiement de mesures de sécurité sans avoir une vision d'ensemble des besoins de l'organisation. » Ainsi, le secteur d'activité d'une entreprise peut comporter des exigences légales et réglementaires bien précises dont il faudra absolument tenir compte dans la mise en place d'un programme de sécurité.

Connaître le contexte légal et réglementaire de l'entreprise constitue donc la première étape de la mise en place d'un programme de sécurité. « Il faut ensuite établir la valeur des informations à protéger », enchaîne Richard Neault. Il est primordial de bien doser les mesures de sécurité en fonction de la valeur stratégique des données et des systèmes que l'on veut protéger. « Par exemple, note Luc Poulin, il est certain que les données contenues dans le dossier médical d'une personne doivent bénéficier d'une sécurité à toute épreuve. À l'opposé, des informations publiées sur le site Internet d'une entreprise n'ont pas besoin du même niveau de protection de confidentialité, puisqu'elles sont déjà publiques. »

Une fois ces étapes franchies, il est temps d'évaluer les besoins en sécurité autant en ce qui concerne directement la quincaillerie informatique que les applications, sans oublier le cadre physique de travail. Richard Neault insiste sur le fait qu'il faut réunir les bonnes personnes pour déterminer ce que l'entreprise veut sécuriser. « Les responsables de tous les secteurs d'activité de l'entreprise sont bien placés pour valider la démarche, explique-t-il. Leur participation est d'autant plus importante que ce sont eux qui appliqueront les mesures de sécurité. »

Richard Neault

C'est seulement ensuite que la dimension technologique peut entrer en jeu. Il faut toutefois oublier la recette miracle. « Il n'y a pas eu d'évolution majeure au cours des dernières années », remarque Gabriel Hébert, ingénieur junior et conseiller en sécurité à l'ISIQ. « Par exemple, en ce qui concerne la détection des logiciels malveillants ou des intrusions dans les réseaux, la technologie est encore principalement basée sur le principe de l'identification de la signature d'un virus ou d'une attaque et l'inscription de cette signature dans un logiciel de détection. » À ce petit jeu, l'industrie peine à suivre les filous de la planète.

Jean-Marc Robert, ing. jr

Gabriel Hébert reconnaît aisément que les moyens technologiques ne peuvent pas pallier tous les risques auxquels les usagers, consciemment ou non, exposent l'organisation. « Il faut que ces derniers comprennent la raison d'être des mesures de sécurité mises en place par l'entreprise plutôt que de les voir comme des contraintes exagérées. »

Tous les intervenants vous diront que « trop, c'est comme pas assez » en matière de sécurité de l'information. L'erreur est souvent de concevoir des procédures de sécurité tellement élevées et lourdes que le système informatique devient pratiquement inutilisable. « De façon très concrète, mentionne Gabriel Hébert, cette lourdeur pourra aussi inciter les usagers les plus futés à trouver des moyens de contourner les barrières. » L'entreprise risque de revenir à la case départ en ce qui a trait à la sécurité.

David Poelhuber

LA SÉCURITÉ DÈS LE POINT DE DÉPART

Bien que la plupart des intervenants déplorent le fait que la sécurité ne soit pas encore bien ancrée dans la culture des organisations, il semble que le vent tourne lentement depuis quelques années. À l'ETS par exemple, on donne un cours obligatoire sur la sécurité des systèmes au premier cycle et à la maîtrise du programme de génie des technologies de l'information. En génie logiciel, il y a un cours optionnel au premier cycle, cours que la plupart des étudiants suivent, selon François Coallier. « À la demande des étudiants, nous avons ajouté un cours optionnel aux deux cycles. De plus en plus, les ingénieurs que nous formons voient la sécurité comme un besoin et une étape indispensable dans la conception. »

Cette attitude commence à poindre dans l'industrie informatique. « Après avoir maintenu une approche réactive, qui consiste à contrer les attaques ou à résoudre les problèmes quand ils surviennent, nous passons progressivement à une approche plus proactive », estime Jean-Marc Robert, ingénieur junior, professeur au Département de génie logiciel et des technologies de l'information à l'ETS.

« Il ne faut pas oublier que l'informatique n'existait pas il y a 60 ans, c'est un domaine relativement jeune », fait valoir Luc Poulin avant d'ajouter que l'industrie de l'automobile est un bon exemple en matière d'intégration de la sécurité à l'étape de la conception. L'image parle d'elle-même. « On ne pourra jamais garantir totalement la sécurité d'une application ou d'un serveur », reconnaît toutefois Jean-Marc Robert.

Comme pour l'automobile, l'approche proactive consiste à concevoir des applications plus robustes. « L'idée centrale est de réduire le plus possible la surface d'attaque en intégrant un nombre adéquat de barrières pour augmenter la robustesse du logiciel », explique Jean-Marc Robert. Le voleur ne s'acharnera pas sur la porte principale s'il peut entrer par une grande fenêtre ouverte à l'arrière de la maison. « Les ingénieurs peuvent jouer un rôle important en intégrant dans les diverses phases du cycle de développement des logiciels des activités ayant pour objectif d'améliorer la robustesse et la sécurité des logiciels produits », croit Jean-Marc Robert.

LE FACTEUR HUMAIN

Au-delà des moyens technologiques, il y a aussi une culture de la sécurité à mettre en place. L'élément humain demeure le maillon faible de la chaîne de sécurité, comme l'illustre ce qu'on observe dans le secteur de l'automobile : les pannes ou les défaillances d'un système de freinage ou d'un boulon peuvent mener à un accident ; or il arrive que celles-ci découlent d'un manque de compétences ou simplement d'une inattention. Les malfaiteurs sont au fait de cette vulnérabilité. « La fraude psychologique, est une des approches les plus fréquentes », précise Richard Neault. Le fraudeur manipule subtilement les gens pour amasser progressivement des éléments d'information sur des employés clés au sein d'une entreprise. La technologie la plus couramment utilisée encore de nos jours est… le téléphone ! Les réseaux sociaux, comme Facebook, sont aussi des lieux propices pour récolter patiemment les informations de base afin d'usurper l'identité d'une personne.

« Les pourriels constituent la principale porte d'entrée des fraudeurs à la recherche de renseignements personnels », nous

prévient David Poelhuber, chef de l'exploitation de Zerospam Sécurité. Un classique : vous recevez un courriel qui vous invite à cliquer sur un hyperlien pour obtenir des photos inédites des funérailles de Michael Jackson. « L'hyperlien conduit à des photos, mais surtout à un site qui contient un logiciel malicieux qui pourra prendre le contrôle de votre ordinateur, envoyer un cheval de Troie ou un ver », explique David Poelhuber. L'escroc joue sur la curiosité naturelle de tout être humain.

« La plupart du temps, note Richard Neault, le volet humain est le plus accessible sur le plan de l'investissement, mais c'est aussi celui qui est mis de côté le plus souvent. Au sein de l'entreprise, utilisateurs, gestionnaires techniciens, ingénieurs, développeurs, bref, tout le monde doit être sensibilisé à la sécurité de l'information : de l'employé au bas de l'échelle jusqu'à la haute direction sans oublier les membres du conseil d'administration. » □

La vérification

Actuellement, l'industrie vérifie la résistance des logiciels et des équipements au moyen de simulations. Or, compte tenu de la multitude des possibilités et des coûts associés à une simulation en profondeur, cette approche ouvre la voie à des défaillances inattendues des systèmes.

Sofiène Tahar, ing.

Pour mieux tester les applications et les équipements, l'ingénieur Sofiène Tahar, professeur à l'Université Concordia et titulaire d'une chaire de recherche de vérification formelle des systèmes sur puces, met de l'avant une approche mathématique basée sur les probabilités. « Beaucoup de systèmes ont des comportements probabilistes, souligne le chercheur. Nous adoptons un raisonnement mathématique pour essayer de prévoir tous les cas possibles. » La méthode formelle appliquée consiste à créer un modèle mathématique qui permet de calculer toutes les probabilités qu'un événement, une défaillance, se produise. « L'approche n'est pas nouvelle, indique Sofiène Tahar, mais nous avons entrepris de l'appliquer à des systèmes complexes. »

L'approche de vérification formelle a déjà permis de détecter une défaillance dans une application de télécommunication industrielle. « Les concepteurs de la puce électronique ne nous croyaient pas, jusqu'à ce que les ingénieurs qui ont développé le code matériel soient eux-mêmes convaincus du problème, se rappelle Sofiène Tahar. Malheureusement, il y avait déjà des milliers d'exemplaires de la puce en circulation. »