La technique ne suffit pas pour traiter des problèmes de sécurité informatique

Par Yvon Klein, Président du CERT-IST

On assiste à une évolution rapide des besoins d'échanges et des usages qui va vers une dématérialisation croissante de l'information et une recherche de continuité de la communication entre les différents modes d'accès à l'information: téléphonie mobile, fixe et connectivité Internet avec ou sans fil. On constate une croissance des menaces et des risques liée à la multiplicité et à la complexité des technologies mises en œuvre, à la croissance du nombre d'usagers, mais aussi à l'évolution des comportements.

On veut accéder à l'information où qu'elle se situe, quel que soit le moyen de communication, le point de connexion ou les réseaux empruntés pour l'atteindre

Les employés d'une entreprise ont de plus en plus besoin d'accéder aux données externes situées sur Internet. A coté de l'utilisation de produits qui sont maintenant considérés comme des outils du monde professionnel : messagerie, transfert et partage de fichiers, travail coopératif, navigateurs et serveurs Web, et les évolutions en cours : vidéoconférence, voix sur IP, …, les personnes ont tendance chercher à reproduire dans l'entreprise, les modes de fonctionnent qu'ils ont déjà adoptés à leur domicile : échanges par messagerie instantanée, échanges " peer to peer ", vidéo, audio, paiements en ligne,…

La flexibilité amène l'entreprise à offrir à ses employés d'accéder aux ressources internes et aux outils métiers depuis différents terminaux (PDA, PC portables, PC fixes) depuis le réseau de l'entreprise mais également depuis les réseaux externes, que ce soit dans des endroits publics ou depuis la sphère privée.

Le développement rapide des services offerts aux particuliers notamment en terme de réseau (ADSL, WiFI) entraîne des modifications de comportement. Le terminal reste connecté en permanence, sans pour autant que le propriétaire ait conscience des besoins de protections contre les menaces : virus, logiciels espion, chevaux de Troie, usurpation, prise en main à distance, écoute, … ni de la nécessité de maintenance des produits installés (mise en place des correctifs, fichiers de signatures, …).

La cyber-criminalité s'adapte

L'élargissement des possibilités d'accès à l'information, ajouté à la prédominance des acteurs essentiellement américains (MicroSoft, Cisco, …) dont nous sommes fortement dépendants et la banalisation des données de l'entreprise (lors de leur mise en place sur les Web internes) ont entraîné une évolution de l'approche des malveillants tant dans la nature des attaques, dans leur comportement, qu'en ce qui concerne les cibles recherchées. Aux actions d'experts très pointus se superposent celles d'amateurs éclairés qui ne font qu'utiliser des informations et des logiciels téléchargeables aisément sur Internet. Les malveillants ciblent les

vulnérabilités des produits diffusés en grand nombre pour obtenir des résultats plus spectaculaires. Les particuliers et les PME moins sensibilisés à la sécurité, et disposant de plus en plus, de connexions quasi-permanentes peuvent devenir des vecteurs involontaires de propagation par rebond. Du fait de la quasi monoculture technique, l'effet " boule de neige " est assuré.

Sans nécessairement constituer une forme de criminalité, certains comportements induisent une pollution qui représente un risque majeur. L'évolution du volume de courrier non sollicité va par exemple obliger les entreprises à se doter de dispositifs anti-spam plus performants afin d'éviter l'engorgement.

La sécurité absolue n'existe pas, la protection doit être multiforme

Les entreprises sont passées d'une approche purement technique du traitement de la sécurité à une approche plus globale intégrant les aspects organisationnels et juridiques, et impliquant de nouveaux acteurs comme les ressources humaines, la Direction de la communication, les Assurances. Les Directions de la sécurité du SI évoluent vers une fonction de Direction de la sécurité de l'information, et se rapprochent de la Direction Générale. On passe du paradigme du statique château-fort : contrôle de périphérie avec des pare-feu, gestion de listes noires, listes blanches, anti-virus, ... à une approche plus dynamique : supervision de la sécurité, IDS, pots de miel, ... pour se donner les moyens de la réaction rapide. La prévention nécessite une anticipation des crises à venir en se préparant à y répondre efficacement, et donc d'avoir au préalable défini l'organisation humaine et technique, les rôles, les procédures, les moyens de communication interne et externes.

La prévention passe par un travail amont sur l'urbanisme des infrastructures techniques de l'entreprises qui devient de plus en plus interdépendant du SI et des réseaux. Il est impératif d'avoir une approche cohérente globale qui intègre la sécurité dans l'ensemble du cycle de vie des services et des produits générés, qu'ils soient destinés à un usage interne ou aux clients. Il est indispensable que les donneurs d'ordre expriment la sensibilité des informations et des ressources qui seront en jeux pour que, à la suite d'une analyse de risque, les processus permettent de décliner les objectifs de sécurité.

On le voit, toutes ces actions ne peuvent être menées en cohérence s'il n'y a pas un fil conducteur constitué par une " Politique de Sécurité de l'Information " portée par les acteurs situés au plus haut niveau de l'entreprise, et des déclinaisons sectorielles et des corpus de règles qui encadrent les actions à mener par les différents métiers de l'entreprise.

L'entreprise doit être alimentée en continue par des informations de sécurité qualifiées

Pour assurer le maintien des infrastructures au bon niveau de sécurité, il est nécessaire d'être en permanence informé des dangers qui pèsent sur les ressources. Cela suppose que l'entreprise soit alimentée en informations pertinentes (avis de sécurité, alertes, fichiers de signatures, correctifs, ...). Le nombre important d'informations qui circulent nécessite que celles-ci soient qualifiées par une entité de confiance. Ce rôle de veille, de validation des sources

et de qualification d'informations est celui des CERT (en France : le CERT-A pour les administrations, le CERT-Renater pour les universités, le CERT-IST pour le monde industriel, des services et du tertiaire).

Ces informations de sécurité doivent de nouveau être analysées selon les métiers et le contexte de l'entreprise de façon à agir à bon escient et à un coût acceptable. Il est par exemple nécessaire de déterminer soigneusement l'opportunité d'appliquer un correctif, mais quand la décision est prise il faut se donner les moyens techniques et humains de le déployer très rapidement partout dans l'entreprise.

Les vers qui se sont propagés en 2003 (Slammer en janvier et Blaster, Sobig, … en août) ont convaincu les derniers réticents qu'il fallait que les entreprises disposent non seulement d'infrastructure anti-virus et d'organisation de traitement des crises efficace, mais aussi de moyens techniques de mise à jour automatique des correctifs de sécurité.

Conclusion

La forte croissance des besoins de communication, et la perméabilité entre le monde du travail et la sphère privée, accroissent de façon très importante les risques qui touchent à l'information et par conséquence aux enjeux économiques des entreprises.

Le traitement de la sécurité nécessite maintenant une forte pro-activité s'appuyant non seulement sur des infrastructures techniques mais aussi sur de moyens organisationnels éprouvés, de disposer d'informations qualifiées et d'impliquer des acteurs qui ne sont plus seulement techniques et qui travaillent en collaboration. La communication que ce soit en interne entreprise ou vers les clients et partenaires devient essentielle.

La mise en œuvre de solutions de sécurité adaptées aux risques et aux enjeux d'une entreprise peut parfois être supérieur à sa capacité d'engagement dans ce domaine. La solution doit passer par la mutualisation des efforts pour pouvoir optimiser le coût des activités de veille et d'alerte permettant de réduire le risque à un niveau acceptable et de disposer des ressources nécessaires d'analyse et d'intervention permettant en cas d'incident ou d'attaque de maintenir pour l'entreprise le service attendu du système d'information.

La sécurité en devenant un argument de vente, va constituer pour le client, un facteur de différenciation entre les entreprises.