INF 1160 – Les réseaux d'entreprise

Politique sur la sécurité du réseau

Termes de référence

Quelques définitions pour parler le même langage

SINISTRES : Événements liés aux caprices de la nature ou aux bâtiments. Ils peuvent affecter lourdement les équipements informatiques ainsi que les informations contenues sur les divers types de supports de données :

– les inondations,

– les incendies ou les dommages causés uniquement par l'eau et la fumée,

– les tremblements de terre,

– les explosions,

– les effondrements.

Il faut vous demander si les locaux contenant des appareils ou des disquettes informatiques se situent dans *une zone de risque*.

ACCIDENTS TECHNIQUES : Accidents relatifs à la technologie et qui pourraient interrompre, pendant un certain temps, et même compromettre sérieusement la poursuite des activités de l'entreprise :

– les bris d'équipement;

– les pannes de courant;

– les interruptions momentanées du fonctionnement du système informatique.

ERREURS : Autre type d'accident relié aux diverses fautes commises par les individus ayant accès aux systèmes informatiques. La malchance, le manque d'expérience ou la négligence peuvent causer les erreurs suivantes :

– les destructions accidentelles d'informations;

– les modifications de programmes ou de données;

– les utilisations non appropriées de l'équipement.

MÉFAITS : Incidents liés à la malveillance d'individus sans scrupules et prêts à tout pour parvenir à leurs fins. En l'absence de moyens de prévention et de détection des situations irrégulières, l'organisation devient une proie facile pour les voleurs et autres fraudeurs.

VOLS et FRAUDES :

– vol des informations confidentielles,

– utilisation de l’ordinateur à des fins personnelles (d’où l’importance d’établir un code d’éthique);

– détournements électroniques de fonds,

– modification des données (sur le personnel, la paye, etc.).

Autres termes : RÉVOLTES, ATTENTATS TERRORISTES, VIRUS.

Document tiré de Microsoft France http://www.bcentral.fr/Solutions/default.asp

Les protections physiques

Plusieurs systèmes permettent de protéger le matériel informatique.

Contre le risque d'incendie, prévoyez des extincteurs, obligatoires dans les lieux publics. Vérifiez quels sont les matériaux de votre bâtiment. Les moquettes et les rideaux sont-ils ignifugés? Y a-t-il des portes coupe-feu?

Contre le vol, assurez-vous tout d'abord de l'état de toutes les huisseries, portes et fenêtres, surtout si vous êtes au rez-de-chaussée. Ensuite, une alarme volumétrique sera souvent la bienvenue et généralement demandée par votre assureur.

En ce qui concerne les appareils, la majorité des unités centrales et des écrans disposent de petits ergots prévus pour recevoir un dispositif de sécurité, un câble en acier le plus souvent. Il en existe même pour les souris, claviers et autres périphériques d'impression ou de stockage de données. Si vos collaborateurs ont des portables, faites-les ranger dans une armoire fermée à clé.

Les boîtes et les CD d'installation des logiciels peuvent également attirer l'attention. Là aussi, mettez-les en lieu sûr, cela vous protégera contre d'éventuels vols et diminuera la tentation de certains d'effectuer des copies illicites.

Les assurances

Si, malgré toutes les précautions prises, le pire arrive, votre assureur est là pour vous dédommager. La plupart des assureurs proposent des options qui couvrent les risques liés à la perte de l'outil informatique, à la destruction de données ou à la cessation totale ou partielle d'activité par suite d’un préjudice.

Néanmoins, pour vous éviter des désagréments supplémentaires ou des surprises sur le montant des remboursements, lisez bien votre contrat d'assurances, et plus particulièrement les points liés au matériel et aux logiciels informatiques, avant de le signer. Attention à la valeur de « remplacement » et à la « vétusté ».

Le matériel informatique se déprécie très rapidement. En six mois, le prix d'un même ordinateur neuf peut avoir chuté de 50 %. Pour vous rembourser, les assureurs se basent parfois, non pas sur une valeur à neuf (comme c'est le cas pour du mobilier par exemple), mais sur une valeur de remplacement. Un Pentium III 500 acheté à prix d'or en 1998 sera alors estimé au prix d'un Pentium III 500 aujourd'hui (même si cela a pratiquement disparu des catalogues). Second piège, le coefficient de vétusté, qui peut aller parfois jusqu'à 70 %.

Lorsque ces deux méthodes sont cumulées, c'est peu dire qu'il reste au final une peau de chagrin...

Malgré tous les moyens de prévention, on ne peut pas toujours empêcher les catastrophes de se produire ni les fraudeurs de s’introduire habilement dans un système. Il faut donc s’assurer que

l’on saura réagir convenablement en cas de problème; il vaut mieux y penser avant qu’après. N’oubliez pas : cela n’arrive pas qu’aux autres!

Audit de sécurité

Entre audits organisationnels et techniques, tests d’intrusion ou simple analyse des vulnérabilités, le terme d’audit est certainement l’un des plus galvaudés du vocabulaire informatique. Pourtant, le véritable audit est une nécessité. Encore faut-il savoir ce que l’on commande.

Un audit de sécurité a pour objectif d’évaluer les risques encourus par le système d’information et de préconiser des parades. Dit comme cela, l’affaire paraît simple. Mais toutes les sociétés de service informatique ne fournissent pas sous ce vocable le même service. Certaines dépêchent un technicien pour installer et configurer un simple pare-feu, tandis que d’autres revendent des tests de vulnérabilités automatisés depuis Internet. D’autres encore se targuent d’ausculter le code source des applications maison, à la recherche de vulnérabilités oubliées par l’équipe de développement. Et toutes appellent cela un audit. Mais qu’est-ce que le véritable audit de sécurité?

L’audit est avant tout une prestation de service interne (acte de service effectué chez le client) par opposition au test, qui se contente de mesurer la perméabilité en périphérie du réseau. Exit donc les tests de vulnérabilités automatisés, et même les tests d’intrusion. L’audit est ainsi l’affaire d’équipes dépêchées sur un site afin de pratiquer des mesures. Même lorsqu’il est dit « technique », l’audit demeure interne : il est réalisé sur la base du code source, et non simplement d’une tentative de compromettre l’application depuis l’extérieur durant son fonctionnement. Autre critère essentiel : l’audit met en lumière des faiblesses et propose obligatoirement des solutions pour chacune d’elles.

L'audit organisationnel : une vue d'ensemble essentielle

La portée de l’audit définit ensuite son type : il sera organisationnel ou technique. Le premier couvre l’ensemble du système d’information de l’entreprise, de son personnel à ses procédures. Le second étudie en détail une architecture particulière (passerelle, interconnexion, application). Il est plus courant de commencer par un audit organisationnel, qui est une mesure globale du système d’information et de ses points faibles.

Commencer par un audit technique, c’est prendre les choses par le mauvais bout. C’est un peu comme écrire une application sans avoir fait un cahier des charges. Il faut prendre un peu de recul par rapport à la sécurité, et avoir déjà défini un référentiel.

La prestation organisationnelle permet ainsi de couvrir l’ensemble du système d’information et d’en identifier les dysfonctionnements et les risques potentiels.

L’audit général, organisationnel, permet de définir ce que l’on veut faire. Il dicte les règles, la politique de sécurité, les normes. Cela donne une « cible » de sécurité, qui peut ensuite servir de mètre étalon lors d’audits successifs.

Concrètement, un audit organisationnel dure entre 20 et 40 jours. Le prestataire dépêche un ou plusieurs consultants chez son client. Après une première série de réunions, chargées de définir le périmètre de l’audit, de nommer des correspondants au sein de l’entreprise et de planifier ses

interventions, l’auditeur commence son travail. Il ne s’agit pas d’une analyse technique, mais plutôt d’un jeu de questions-réponses : qui s’occupe des sauvegardes? Comment sont-elles planifiées? Qui a accès à la salle des serveurs? Combien de jeux de clés existe-t-il? Qui les détient? Qu’est-il prévu en cas de panne de courant? Ces questions sont classées par thèmes (sécurité physique, contrôle d’accès, sabotage, pannes, erreurs humaines, etc.). L’auditeur ne les invente pas : elles proviennent d’une méthode d’audit reconnue, dite « formelle » (Marion, Mehari, Melisa, Ebios). En intégrant ensuite les réponses au moteur d’évaluation de la méthode (sa « logique »), l’auditeur obtient une mesure de la sécurité du système d’information de l’entreprise, et peut alors proposer des parades aux risques jugés les plus critiques, selon différents scénarios de crise.

Savoir là où ça fait mal

Mais ces méthodes sont lourdes, contiennent des milliers de questions dont toutes ne sont pas applicables dans le contexte de l’entreprise auditée et, surtout, qui demanderaient des mois de travail si elles devaient toutes être posées. La PME ne peut se les offrir et, d’ailleurs, la majorité des questions ne la concerne pas. C’est donc au prestataire de faire un tri, et de ne sélectionner qu’un sous-ensemble adapté au métier de l’entreprise. C’est ici que se fait la différence entre deux auditeurs et c’est ici aussi que naissent des méthodes dites propriétaires ou adaptées.

En PME, ce que les clients veulent, c’est du concret rapidement. L’objectif est d’obtenir en un laps de temps restreint une visibilité des risques et un plan d’action. C’est pour cela aussi qu’il faut savoir adapter la méthode sinon, on peut y passer six mois. Il faut donc identifier les priorités spécifiques à l’entreprise. Les PME sont très pragmatiques, elles veulent des réponses efficaces : savoir là où ça peut leur faire mal. Elles se moquent de savoir si elles répondent à des standards, telle la norme ISO. L’audit de sécurité dit « organisationnel » s’adapte donc aujourd’hui aux PME, qui ont poussé à plus de pragmatisme : les méthodes formelles, lourdes, qui ont donné à l’audit sa réputation de prestations réservées aux grands comptes, ne servent plus que de base.

Le référentiel de sécurité ainsi créé est un document vital : il s’agit du mètre étalon garant du niveau de sécurité de l’entreprise dans le temps.

Les 10 commandements de la sécurité

Créez des mots de passe qui sont faciles à mémoriser par vos collaborateurs et difficiles à découvrir.

Placez un double de vos sauvegardes quotidiennes dans une pièce à l'épreuve du feu et des dégâts des eaux.

Essayez vos sauvegardes pour vérifier qu'elles sont complètes et utilisables.

Éteignez vos ordinateurs individuels, afin de les rendre inaccessibles, quand vous partez déjeuner et fermez vos bureaux.

Équipez vos ordinateurs portables d'un système de verrou physique et de contrôle d'accès aux données qui les rendent inutilisables en cas de perte ou de vol.

Testez les logiciels et les fichiers en provenance de l'extérieur à l'aide d'antivirus mis à jour

toutes les semaines.

Sécurisez vos connexions à Internet, à l'aide d'un coupe-feu par exemple.

Avant d'effectuer des transactions bancaires sur Internet, évaluez le mode de sécurisation proposé par le site marchand.

Désignez une personne responsable de la sécurité dans votre entreprise.

Disposez d'un plan de secours immédiatement opérationnel en cas de sinistre par virus, intrusion, erreur de manipulation, incident technique, etc.

Autre version des 10 conseils pour optimiser sa sécurité :

1. Inciter ou obliger les employés à choisir des mots de passe qui ne soient pas évidents à trouver.
2. Exiger des employés qu'ils changent leurs mots de passe tous les 90 jours.
3. Vérifier que l'abonnement à la protection antivirus est à jour.
4. Sensibiliser les employés aux risques relatifs à la sécurité des pièces jointes aux messages électroniques.
5. Mettre en œuvre une solution de sécurité du réseau complète et adéquate.
6. Évaluer régulièrement l'infrastructure de sécurité.
7. Supprimer immédiatement les droits d'accès au réseau d'un employé quittant la société.
8. Si des employés sont autorisés à travailler à distance, mettre en place un serveur sécurisé et géré de façon centralisée pour le trafic distant.
9. Mettre à jour régulièrement le logiciel du serveur Web.
10. Ne pas exécuter de services de réseau superflus.