

COMPTE-RENDU

Pour son dernier rendez-vous de l'année 2002, le FORUM TELECOM de la SPI+ a consacré la conférence du 10 décembre au thème de la sécurité informatique. Quatre orateurs se sont succédés pour aborder un point précis de cette problématique ou témoigner de leur expérience.

Le FORUM TELECOM a déjà, à plusieurs reprises, organisé des conférences d'information et de sensibilisation sur ce sujet, mais il est apparu de plus en plus évident qu'il nous fallait renouveler ces initiatives pour essentiellement deux raisons. Tout d'abord parce que les entreprises n'ont cessé d'intégrer toujours plus les nouvelles technologies au sein de leur environnement, rendant cet environnement toujours plus sensible et les obligeant donc à toujours apporter plus d'attention au problème de sécurisation. Ensuite, parce que nous avons fait l'objet – probablement à cause des raisons soulignées - de nombreuses sollicitations nous demandant de ré-aborder la question de la sécurité.

Didier GODART, consultant en sécurité informatique, a débuté par un exposé intitulé "Sécurité informatique : Risques, stratégies et solutions". Il a commencé par poser la question "Pourquoi parler de sécurité ?" Avec le développement d'Internet et des réseaux, cette question prend beaucoup d'importance. Dans le monde des affaires, la confiance est importante, elle est la base des relations entre l'entreprise, le marché et les clients. Veiller à la sécurité permet de maintenir la confiance entre ces différents partenaires.

La sécurité permet parallèlement, souligne M. GODART, la protection de la réputation de l'entreprise, d'éviter les pertes financières et de satisfaire aux exigences légales et d'assurances.

L'orateur a poursuivi en donnant une définition de la sécurité "ensemble des mesures permettant d'assurer la protection des biens et des valeurs". Parmi les biens à protéger, on trouve les données informatiques et les systèmes permettant de traiter, de stocker et de gérer l'information.

Au niveau des PME ou des administrations, contre qui doit-on plus particulièrement se protéger ?

L'orateur a présenté deux types de menaces :

- Les menaces externes. Ce sont les pirates, les saboteurs, les concurrents, les anciens employés, les organisations criminelles, etc. ;
- Les menaces internes. Il s'agit des menaces les plus importantes. On y trouve les employés mécontents, les fraudeurs, les complices, les espions et les employés innocents. Il est possible de distinguer deux sous-catégories supplémentaires dans les menaces internes, souvent d'ailleurs négligées :
 - Les travailleurs internes qui travaillent à l'extérieur. Par exemple, le télétravail ou les déplacements professionnels. Le cas des portables non sécurisés reconnectés sur le réseau de l'entreprise est un exemple de mauvaise gestion de la sécurité ;
 - Les travailleurs externes qui interviennent au sein de l'entreprise. Par exemple, les compagnies de nettoyage, les compagnie de maintenance, les déménageurs, etc.

Didier GODART ajoute deux distinctions supplémentaires : les événements volontaires (actes malicieux) et involontaires (événements accidentels comme l'oubli d'une mise à jour de l'antivirus ou d'un backup par exemple).

Jusqu'où faut-il se prémunir contre ces événements ? Tout cela dépend de l'environnement de l'entreprise et de ses exigences. Elle doit pour cela définir ses besoins en sécurité en passant par une

Risques informatiques :

10/12/2002

Quelle politique de sécurité au sein des PME ?

© FORUM TELECOM® SPI+

procédure de gestion des risques. Il s'agit d'abord d'estimer le niveau du risque, l'impact sur l'entreprise, la probabilité qu'il survienne et la faisabilité d'un projet de sécurisation efficace. L'orateur a rappelé que la mise en place d'un système de sécurité compte de nombreuses mesures, qui font appel à différents départements de l'entreprise.

Il a terminé en présentant les éléments à considérer pour déterminer des mesures de sécurité applicables.

Tout d'abord il faut examiner les contraintes liées à l'environnement :

1. le budget octroyé,
2. l'environnement technique,
3. les ressources disponibles,
4. la politique de sécurité de l'entreprise,
5. les nouvelles vulnérabilité introduites.

Ensuite, il faut se poser les questions permettant de cibler une solution précise :

1. Quel problème la solution permet-elle de résoudre ?
2. Comment peut-elle résoudre le problème ?
3. Quels autres problèmes permet-elle de résoudre ?
4. Quels nouveaux problèmes la solution engendre-t-elle ?
5. Quel est son coût ?
6. Vaut-elle son coût ?

L'implémentation de la solution retenue pourra être réalisée de trois manières : soit avec des ressources internes, soit avec l'utilisation de ressources externes, soit en utilisant la technique de l'outsourcing. Dans ce dernier cas, M. GODART rappelle qu'un audit de la société en charge de l'hébergement s'avère nécessaire.

Eric LAPAILLE, le deuxième orateur, s'est attardé sur la sécurisation des réseaux et des connexions permanentes et a présenté les 11 points à prendre en considération pour développer un système sûr.

1. La méthodologie : il faut établir une méthodologie qui permette pour chaque type d'attaque d'avoir une réponse. Le principe de base est de toujours se mettre à la place du hacker pour tester son infrastructure.
2. L'authentification : le mot de passe doit faire l'objet d'une attention particulière. Il existe de nombreux outils pour tester leur "solidité" et les "renforcer", notamment sur le site l0pht.com.
3. Le Firewall : l'adoption d'un Firewall est nécessaire. Il faut être particulièrement attentif à sa sélection mais aussi à sa configuration. L'orateur recommande l'utilisation du système d'exploitation Linux, qui – en plus d'être libre – permet l'accès à un grand nombre de Firewalls.
4. La détection d'intrusion : il existe de nombreux logiciels de détection d'intrusion qui permettent de surveiller l'activité réseau. Si certains estiment que lorsqu'un détecteur d'intrusion réagit, c'est qu'il est trop tard, l'orateur pense de son côté que ce n'est pas vrai dans de nombreux cas. Il est donc préférable d'avoir un tel logiciel installé sur sa machine.
5. La lutte contre les virus : outre les traditionnels antivirus, l'orateur a présenté divers outils existant sur le Net qui permettent de lutter contre les attaques virales ainsi que d'autres

- solutions permettant l'activation de plusieurs antivirus sur une machine. Il a appelé à la prudence lors de la réception de Mail fragmentés pouvant contenir un code malicieux.
6. La politique de sécurité : il est important d'établir des règles pour veiller à la sécurité du réseau d'une entreprise. Quatre points à prendre à compte : la gestion, la sécurisation, le monitoring et l'audit du système informatique.
 7. Le test de vulnérabilité : l'orateur a expliqué que pour vérifier la solidité de son système, la meilleure solution consiste à s'attaquer soi-même, à prendre la place du hacker. Il a présenté des outils gratuits disponibles en ligne permettant de tester sa vulnérabilité.
 8. L'encryption : un des problèmes d'Internet, c'est la possibilité d'usurper une identité afin d'obtenir des informations illégalement (problème que l'on peut contrer grâce à un certificat d'authenticité) mais aussi la capacité de certains à capter des informations y circulant. Il est dès lors nécessaire de crypter les informations sensibles grâce aux protocoles existants (SSL, tunnel VPN, etc.).
 9. L'administration système : la sécurité passe par une surveillance efficace de son système informatique. Que ce soit au niveau de la bande passante utilisée, des connexions actives ou du niveau du trafic.
 10. Le filtrage des contenus : la sécurité et le fonctionnement d'un réseau dépendent aussi des informations échangées. Le responsable d'un réseau doit veiller par exemple à éviter l'échange de fichiers de grande taille qui pourrait saturer la bande passante, etc.
 11. Plan de réponse en cas d'incident : il faut avoir une solution en cas de problème. Trop souvent, l'appel à un professionnel se fait trop tardivement, quelques fois les dégâts ont même été aggravés par des manipulations maladroitement.

Eric LAPAILLE a clôturé l'exposé par la présentation d'une série de liens relatifs au problème de la sécurité informatique.

Le troisième intervenant, **Stany WYRZYKOWSKI**, a abordé le problème des virus informatiques. Il a défini un virus comme étant un programme caché, auto-multiplicateur et qui déclenche une action.

Il existe quatre types de virus.

1. Les virus d'amorce : ils infectent le boot sector du disque dur et remplacent l'amorce du système par ses propres données. Le virus se trouve ainsi chargé en mémoire dès le lancement du système d'exploitation d'un ordinateur. Ce type de virus se rencontre de moins en moins.
2. Les virus d'application : il s'agit ici de programmes qui infectent les fichiers exécutables (spécialement les fichiers avec extension .exe, .com ou .sys). Le code d'amorce est remplacé par le code du virus qui permet son exécution. Ce genre de virus est également de moins en moins utilisé.
3. Les virus macros : ces virus détournent les fonctionnalités offertes par les programmes Microsoft Office (Word ou Excel notamment) pour que leur code soit exécuté. Ils sont la plupart du temps écrits en Visual Basic pour Application, le langage de programmation de Microsoft.
4. Les virus Mail (également appelés vers) : ils s'agit des virus les plus actifs actuellement. Ils utilisent les logiciels de messagerie, et plus particulièrement le carnet d'adresses, pour se reproduire. Les plus sensibles à ce genre de virus sont les programmes Microsoft Outlook et Outlook Express. Certains de ces virus peuvent également cacher leur code dans une page Web.

A côté de ces quatre types de virus, l'orateur a mis en avant ce qu'il appelle les "cousins des virus" :

1. Les Hoax (ou canulars en français) : il s'agit de rumeurs dont le but est de faire croire à la présence de virus. La transmission de messages reprenant la rumeur fait de leur auteur un acteur de sa propagation.
2. Les troyens (ou chevaux de Troie ou Trojans) : ils s'agit ici de véritables programmes qui n'ont pas vocation à se reproduire comme les virus. Ils ont pour objectif d'ouvrir des voies d'accès sur un ordinateur afin de permettre sa prise de contrôle à distance. Ce principe est également utilisé par certains services techniques pour travailler à distance sur des ordinateurs en panne.
3. Les bombes E-Mail : ce type de pratique consiste à utiliser "discrètement" votre ordinateur pour envoyer de manière massive des données informatiques (paquet IP) ou des E-Mail à un destinataire également ciblé par d'autres utilisateurs.
4. Les espions : ce sont de petites applications qui accompagnent souvent les logiciels utilitaires gratuits et qui envoient à des agences de marketing ou de publicité des informations sur les sites visités, les habitudes de surf, etc.

Après cette typologie, M. WYRZYKOWSKI a expliqué le fonctionnement d'un virus. Il a fait l'analogie avec un virus biologique : il se dissimule, il cherche à infecter le plus possible et il modifie une partie des "programmes" existants, dans le cas de l'ordinateur : les commandes, le BIOS, etc.

Il a ensuite présenté les règles générales de protection :

- Faire des copies de sécurité,
- Ne pas télécharger des programmes d'origine douteuse,
- Se méfier des fichiers joints dans les E-Mail,
- Ne pas utiliser de disquettes ou de CD d'origine inconnue,
- Toujours analyser un fichier avec un antivirus avant de l'ouvrir,
- Créer une disquette de démarrage,
- Se tenir au courant des apparitions de nouveaux virus,
- Installer et mettre à jour un anti-virus.

Pour clôturer son exposé, l'orateur a présenté cinq règles à suivre en cas de contamination :

- Installer un logiciel antivirus,
- Mettre à jour le logiciel antivirus,
- Vérifier qu'il ne s'agit pas d'une rumeur,
- Télécharger le remède sur le site d'un développeur d'antivirus,
- Récupérer les données à partir de la sauvegarde.

Francis THIELEN a mis fin à la conférence par son témoignage d'expert en matière d'Internet auprès de la police judiciaire et des tribunaux et de créateur de fournisseur d'accès à Internet. Selon lui, les fournisseurs de services peuvent se révéler le point faible dans un système de sécurité. Il a notamment recommandé le recours plus systématique au cryptage des données confidentielles.