



Sécurité du SI

La SÉCURITÉ DU SYSTÈME D'INFORMATION (SI), tout le monde en parle mais peu maîtrisent ses véritables enjeux. Trop souvent les mots « firewall, antivirus, antispyware, antispam » suffisent à apaiser les esprits.

De nombreuses études (www.HSC.fr) révèlent que :

- 1) Lorsqu'un acte de malveillance est subi par une entreprise cela engendre soit directement, soit indirectement des pertes financières catastrophiques, une image client/fournisseur dévalorisée et un impact négatif sur l'inconscient de vos équipes ;
- 2) La simple présence de matériel de « sécurité » n'a aucune efficacité réelle. Il est faux et très dangereux de penser être sécurisé par la simple présence d'un élément de sécurité statique (boîte, logiciel, etc.) Car votre SI évolue, se modifie, ainsi l'ensemble des éléments attachés à ce dernier doivent évoluer avec lui;

C'est pourquoi les éléments suivants doivent vous sensibiliser à la mise en place d'une politique de sécurité active de votre système d'information : l'évolution des technologies, la découverte quotidienne de nouveaux virus, le temps perdu à éliminer les courriers indésirables (Spam, junk mail), Le relais par votre réseau pour produire des attaques sur des tiers, le suivi de vos sauvegardes et tentatives régulières de récupération des données. Vous êtes vous déjà posé ces deux questions « Combien coûterait la paralysie partielle ou totale de mon système d'information sur 24H ? », « En tant que Responsable du Système d'Information ai-je bien prévenu ma direction des risques encourus en cas de sanction ? »

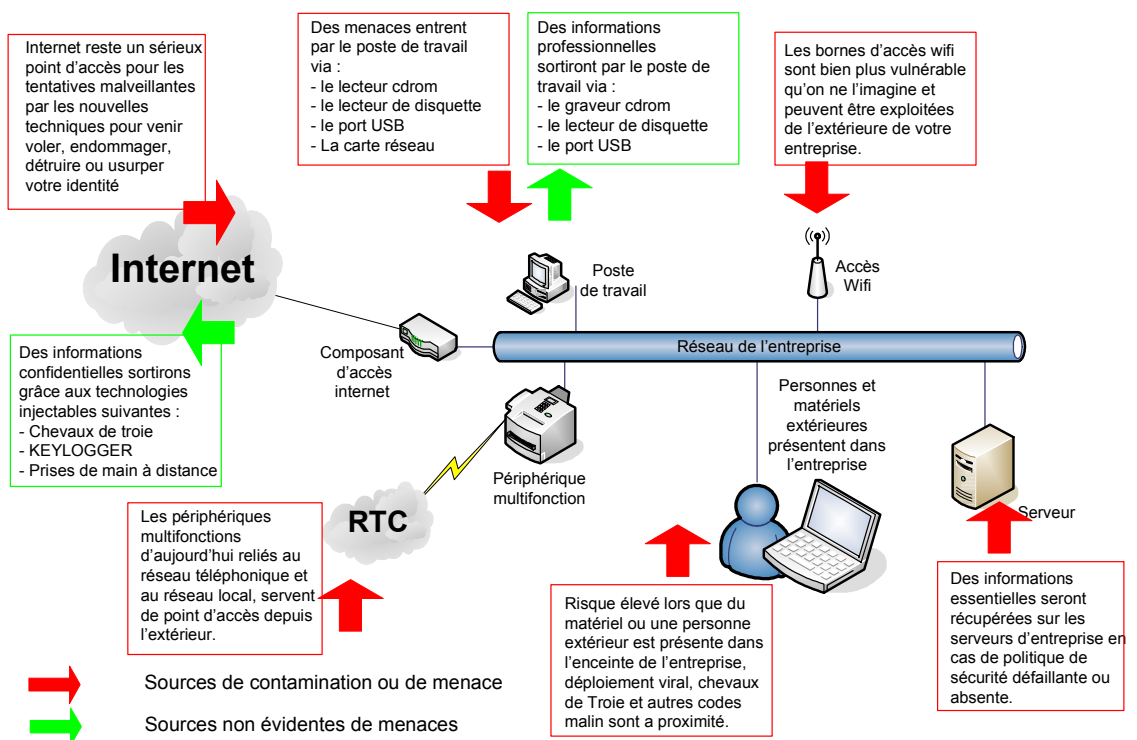


Schéma 1 - Sources de contamination ou de menace

L'objectif d'Archi.Net est de vous aider à mettre en place une politique de sécurité de votre SI. Afin que vous n'ayez plus à vous soucier des conséquences qu'impliquerait la paralysie de ce dernier.

ARCHI.NET envisage la « SÉCURITÉ » comme : *L'optimisation du rapport entre, votre besoin de protéger votre exploitation et votre besoin d'échange pour votre fonctionnement/productivité. Avec en toile de fond une politique visant à parfaire la prise de conscience et l'éducation de chaque utilisateur.*

Ensuite, ARCHI.NET s'est doté d'une méthodologie qui a fait ses preuves et qui est reconnue par toutes les instances. ARCHI.NET propose donc, pour répondre à vos attentes et interrogations, deux types d'audits afin définir les outils et procédures à mettre en place.

L'AUDIT ORGANISATIONNEL est le plus abstrait, mais aussi le plus important car il caractérise et représente les flux d'information ainsi que les chemins empruntés, Il permet par conséquent d'orienter les choix stratégiques concernant la politique de sécurité nécessaire à votre Système d'Information.

L'AUDIT TECHNIQUE est quant à lui une critique structurelle et architecturale, suivi de préconisations pour permettre la convergence de votre besoin d'information et la réponse aux technologies actuelles.

L'audit organisationnel permet :

- De qualifier les flux d'informations de vos métiers ;
- De superposer l'organigramme et les flux d'information ;
- De maîtriser les flux de l'information au sein de votre entreprise ;
- D'apposer les bases des certifications du type ISO 17799 et autres ;

L'audit technique permet :

- De réaliser un état des lieux : Firewall, Virus, Spam, Spyware, Sauvegarde, Messagerie, etc.
- Analyse approfondie ;
- Schématisation du tout courant ;
- De définir les matérielles/logicielles ;
- Mise en place des préconisations ;

Le suivi des mises en place permet :

- Une parfaite maîtrise des vos flux d'information ;
- Une mise à l'épreuve régulière;
- Une correction de la dérive, entre préconisations et habitudes de travail ;
- Une adaptation corrective ou préemptive compte tenu de l'évolution des technologie malveillantes ;
- Une adaptation corrective ou préemptive compte tenu de l'évolution de la société.

Pourquoi une stratégie de sécurité :

- Éviter la fuite/vol/perte/altération de l'information ;
- Pour optimiser votre retour sur investissement ;
- Protéger vos secrets de fabrication et/ou vos avantages concurrentiels ;
- Prévenir une paralysie de la production (Pallier à une rupture matérielle ou un risque : incendie, vol, orage, inondation, etc.) ;
- Présence opérationnelle, Qualité et suivi de services ;
- Concilier votre Système d'information et le risque juridique ;

NOS CLIENTS ONT DÉJÀ CAPITALISÉS SUR NOTRE PROFESSIONNALISME, POURQUOI PAS VOUS ?

Votre contact Local :

Martial LILLO

33, Avenue du Maréchal JOFFRE

60500 CHANTILLY

tel : +33 344 546 071

fax: +33 344 576 813

Courriel: commercial@archi-networks.com