Assises de la sécurité 2005: indicateurs et gestion de risques

La qualité des ateliers, dans leur ensemble, était bonne voire très bonne. En voici quelques échantillons:

Repousser les attaques de type « déni de service » L'atelier organisé par **Radware** sur les « déni de services » a permis une bonne mise à jour de ce dossier. Grâce à sa maîtrise du sujet, le conférencier a su s'adapter à l'auditoire qui n'avait pas forcément une connaissance fine des méandres du protocole TCP/IP. En se basant sur des exemples très concrets, ce expert de Radware a récapitulé les techniques du «**Syn Flooding**» et autres « dénis de services applicatifs » avec beaucoup de pédagogie. Son enchaînement, logique, a passé en revue les modes de protection qui consistent par exemple à limiter la bande passante autorisée pour l'attaquant ou l'utilisation d'un frontal permettant de ne transférer les connexions au serveur cible que dans le cas où elles sont valides (applicatif *statefull*). **Comment intégrer des indicateurs de sécurité dans les SLA de nos fournisseurs ?** Telindus a apporté de nombreux éléments de réponse en proposant notamment un classement des indicateurs par famille (niveau de sécurité, conformité, événementiel, change control/change management). Un modèle pour la consolidation de ces indicateurs sous forme de **tableau de bord** est venu clore la présentation. Ce type de tableau de bord permet d'avoir une idée de la tendance, de réagir ou d'anticiper toute dérive. Il nous donne enfin l'assurance que le partenaire choisi est conforme à nos attentes et que nous pouvons lui accorder notre confiance pour construire avec lui les protections nécessaires pour sauvegarder le patrimoine informationnel de nos sites. **L'analyse et la gestion des risques**

McAfee a donné en 10 points clés une méthodologie d'**analyse des vulnérabilités** et de gestion des risques grâce à une « checklist » particulièrement pertinente. Le conférencier a rappelé la nécessité d'évaluer les contre-mesures par des tableaux de bord compréhensibles par le « top management » car -a-t-il souligné- «*plus les investissements sécuritaires sont efficaces moins on est capable de les justifier*». **La stratégie de Microsoft** L'éditeur de Redmond a exposé sa stratégie de sécurité en faisant **amende honorable** du passé pour aller « vers une informatique de confiance… » Les points de suspension signifiant que c'est un objectif qui n'est pas encore atteint. Une véritable révolution culturelle est en marche, Microsoft ayant dû «**se réinventer en terme de sécurité**». Rendons hommage à l'éditeur car les progrès sont bien réels. Par ailleurs, le partenariat de Microsoft avec la police et la gendarmerie afin de traquer les « botnet » démontre la réelle implication de Microsoft dans la lutte contre la criminalité informatique. **Le risque juridique lié au système d'information par Jean Marc Chartres (Telindus)** Le conférencier, par sa bonne maîtrise du sujet, a fait quelques rappels essentiels sur les **devoirs de l'entreprise** en matière de protection des et des données nominatives. La vulgarisation des articles du code civil, pénal, droit du travail et autre LEN nous a permis de mieux évaluer la mission juridique du RSSI ainsi que ses limites, devoirs et droits. **Et la sensibilisation ?** À signaler, l'excellent outil baptisé **Secureman d'Aequalis**: c'est un quiz ludique en ligne au format flash qui éduque et responsabilise les utilisateurs. Une façon de sensibiliser un large public, novices et béotiens compris, à la sécurité. **Rugby et sécurité informatique : même combat selon Brother, sponsor du stade Français** Complètement décalé, direz-vous ? Eh bien non ! Une explication de texte fournie par Fabrice Landreau, ex-international et

co-entraîneur du Stade Français, a permis de prendre conscience des valeurs communes du Rugby et de la sécurité informatique. En effet, la solidarité devant une attaque, la lucidité, la discipline, le partage des connaissances? autant de valeurs fondamentales que l'on retrouve dans le sport mais aussi dans le quotidien des RSSI qui luttent contre un adversaire virtuel de plus en plus aguerri aux méthodes de protection. **Le CIGREF: risque et gouvernance** Un représentant du CIGREF a expliqué avec beaucoup d'humour la place de la gestion des risques dans la gouvernance du SI. La gouvernance n'est pas un projet, c'est un ensemble de processus permettant d'équilibrer la création de valeurs et de performance et la réduction des risques. **La place de l'intelligence économique en France** Disons-le, nous avons été « époustouflés » par l'exposé d'un ancien haut fonctionnaire sur les problématiques d'intelligence économique et les solutions pratiques pour sa mise en oeuvre. Pas de 'slides', ni de beaux schémas '.ppt' colorés, juste une synthèse brillante d'un orateur dont toute la salle a bu les paroles, tant il a été convaincant en nous soulignant entre autres que nous, Français, devions évoluer vers un **décloisonnement de l'information**. Une information non partagée est inutile. « *A faire de la rétention d'information, nous mourrons seuls avec nos secrets!* a-t-il martelé. Faut-il alors instituer un « Monsieur » intelligence économique dans les sociétés ? La réponse se dirige plutôt vers l'émergence d'un comité spécialisé. Dans le cas contraire, nous retomberions aisément dans le travers mentionné. **Rencontres & échanges autour d'activités ludiques** Comme il est de tradition aux assises de la sécurité, le dernier jour est consacré à la détente. Cette année, les invités ont pu goûter aux joies du modélisme à travers le pilotage de voitures et de voiliers radiocommandés. Bien que la pluie se soit invitée à ce moment de détente, il s'agit d'une période propice aux rencontres, aux échanges et débats constructifs. **Bernard Foray** pour **Vulnerabilite.com.**