

Forum Eurosec : La sécurité sans frontières face une criminalité sans limites Emmanuelle Lamandé - Mag Securs

Andrea Servida, directeur de l'unité « Internet, réseaux et sécurité de l'information » à la Commission Européenne, a eu la lourde tâche d'ouvrir la 18ème édition du forum Eurosec, qui s'est tenu à Paris Cap 15 du 23 au 25 mai 2007. A l'occasion d'une première table ronde sur la sécurité sans frontières, il a mis l'accent sur la dépendance de la société envers les nouvelles technologies, le besoin d'ouverture des frontières, ainsi que sur la nécessaire collaboration internationale dans la guerre contre le crime informatique, qui lui est sans limites.

La stratégie développée par la Commission Européenne depuis 2001 doit, selon Andrea Servida, être revitalisée en revoyant la situation NIS (Network Information Service) ainsi que les challenges posés par la convergence des technologies, notamment du fixe et du mobile. L'objectif poursuivi réside dans la continuité et la sécurité des services, ainsi que l'intégrité et la confidentialité des données. Andrea Servida souligne, de plus, la nécessaire prise de conscience du besoin de sécurité. Chacun doit prendre ses responsabilités. Quatre pôles représentent, selon lui, les clés principales pour améliorer et développer une culture NIS : la technique, l'économique, le social et le légal. Pour le futur, la commission souhaite renforcer la collaboration, qui reste insuffisante à ce jour, par le biais de partenariats nationaux et internationaux. Il faudra également mieux définir les responsabilités des développeurs de logiciels et des fournisseurs d'accès à Internet. « Tant que les choses ne nous atteignent pas directement, on ne se sent jamais vraiment concerné »

Christian Ehlers Mikkelsen, Devoteam Consulting, rejoint Andrea Servida sur cette notion de dépendance, l'utilisation d'Internet étant de plus en plus courante et intégrée dans la majeure partie des sociétés et services actuels. Cet engouement sur la toile est devenu un marché juteux pour les hackers, qui en font aujourd'hui un véritable business. Prévenir les risques et en sécurisant son système est donc devenu une priorité, cependant « tant que les choses ne nous atteignent pas directement, on ne se sent jamais vraiment concerné », souligne-t-il. Kim Aarenstrup, ISF (Information Security Forum) établit un tour d'horizon, une prospective de ce qui risque d'arriver dans les deux à trois prochaines années en termes de menaces. Il distingue cinq facteurs qui représentent le monde et son évolution : le politique, l'économique, le légal, le socio-culturel et le technique. A travers son scénario, il imagine une perte des liens de communication, où l'infrastructure serait fréquemment dérégulée et le terrorisme permanent. Au niveau légal, il souligne une forte croissance en terme de conformité pour répondre aux lois et réglementations de plus en plus coercitives. Négliger les risques opérationnels risque de produire des accidents. En même temps, moins de risques menace de diminuer notre attention. Au niveau économique, le crime organisé poursuit un objectif financier, puisque aujourd'hui les hackers agissent pour la rente. « Nous surestimons trop souvent les changements qui auront lieu les deux prochaines années et nous sous-estimons les dix prochaines »

La collaboration sera nécessaire entre la police traditionnelle et la police spécialisée dans le high tech. L'objectif étant, pour Kim Aarenstrup, d'arriver à un « high risk staff ». Au niveau socio-culturel, on observera, selon lui, la convergence entre le téléphone, l'ordinateur, l'ipod. En termes techniques, l'adaptation du système RFID nécessitera un système de lutte, de contrôle beaucoup plus strict. Pour conclure, selon Kim Aarenstrup, « nous surestimons trop souvent les changements qui auront lieu les deux prochaines années et nous sous-estimons les dix prochaines ». Pour Patrick Pailloux, SGDND, le simple arrêt des systèmes informatiques a des conséquences très importantes, car rien de ce que nous faisons à l'heure actuelle ne dépend d'un système d'information. Les conséquences constatées aujourd'hui restent cependant économiques, puisqu' aucune des attaques recensées à ce jour ne s'est avérée mortelle. En matière d'attaques, on constate un très grand nombre d'attaques en France avec une très forte croissance pour le défacement de sites : en 2006, 2400 sites ont été défigurés. De plus, Internet est devenu un outil de protestation. Le déni de service, par exemple, est une sorte de « sitting » sur Internet. Rien de ce que nous faisons à l'heure actuelle ne dépend d'un système d'information

Le phishing reste toutefois l'attaque la plus signalée en France ; elle touche principalement les banques et de plus en plus de sites de e-commerce. Les botnets, quant à eux, représentent le troisième type d'attaque qui touche le plus les particuliers. On retrouve également différentes méthodes : faux messages, publicité, clés USB abandonnées... En outre, les attaques ciblées restent indétectables par les systèmes classiques de pare-feux et sont de plus très peu signalées. Ce tableau dressé par Patrick Pailloux se base sur des statistiques nationales, cependant ce qu'il dévoile ne s'apparente en aucun cas à un phénomène national, dans le sens où il touche tout le monde. La langue peut néanmoins poser problème car dans certains cas pour mener à bien une attaque, il faut maîtriser la langue. Il faut coordonner les différents ministères

Face à ce constat, Patrick Pailloux s'est intéressé au rôle de l'état dans ce domaine. Que font les états ? Quelles responsabilités ? Ils doivent à la fois protéger leur propre SI et essayer de promouvoir les bonnes pratiques, les échanges. Il faut se préparer au pire mais surtout se poser les bonnes questions : fait-on assez de contrôles ? Il faut aller dans le sens d'une coordination entre les différents ministères, créer un centre opérationnel des SI (gestion de crise, veille, alerte.). Des exercices

Date: 30/05/2007

OJD:

Page: 1

Edition:(FRA)

Suppl.:

Rubrique:

mag-securs.com

nationaux sont réalisés en guise de tests. Ce type d'actions s'avère toutefois très complexe car il est extrêmement difficile d'arriver à quelque chose de réaliste, dans le sens où une coupure du réseau est impossible. Chacun a un rôle à jouer dans cette lutte. L'état seul ne peut pas être efficace. La sécurité nécessite une coopération étroite et active entre les acteurs, et de plus sans frontières. A l'heure actuelle, les frontières représentent un frein majeur dans cette lutte. Face à une cybercriminalité sans frontières et sans limites spatio-temporelles, les réglementations internationales sont beaucoup trop disparates pour être efficaces. Emmanuelle Lamandé - Mag Securs < article précédent mai 2007

<http://www.mag-securs.com/spip.php?article8378>