

La sécurité tient salon à l'Eurosec 2007

Rendez-vous annuel des professionnels de la sécurité des systèmes d'information, l'Eurosec vient de refermer ses portes. Continuité d'activité, cyberterrorisme, dissection d'attaques... reportage.



Parmi les nombreuses thématiques abordées à l'occasion de la seconde journée de cette 18e édition du forum Eurosec 2007 : la continuité d'activité, l'intelligence économique, le terrorisme, l'analyse de code malveillant et d'attaque *man-in-the-middle*, ou bien encore l'économie du spyware.

Sensibiliser les entreprises au terrorisme



"Terrorisme et nouvelles technologies"

Jean-Louis Bruguière, vice-président du Tribunal de Grande Instance de Paris © Journal du Net / Cécile Debise

Le terrorisme ne relève plus de la sphère exclusive des états et de la sécurité nationale. C'est le célèbre juge français et désormais vice-président du Tribunal de Grande Instance de Paris, Jean-Louis Bruguière, qui le déclare en préambule de la conférence lançant la seconde journée du salon Eurosec 2007.

Le terrorisme, et l'usage qu'il peut faire des nouvelles technologies, intéresse toutes les sphères, ou du moins le doit-il, incluant de fait les acteurs du monde économique que sont les entreprises. Polymorphe, le terrorisme joue en effet contre elles en générant de l'instabilité, notamment économique.

Les terroristes font un usage opportuniste des nouvelles technologies, estime Jean-Louis Bruguière. Il insiste toutefois sur leur haut niveau de compétence et la sophistication de leurs procédés. Leur usage du chiffrement, notamment via PGP, et de la scanographie, complique d'ailleurs l'infiltration et le démantèlement des réseaux.

Pour les entreprises, la prise en compte de la variable terrorisme s'intègre désormais à la politique de gestion des risques, dans un contexte d'économie mondialisée. Le but de son intervention, se

défend Jean-Louis Bruguère, n'est pas d'alarmer, bien au contraire, mais d'informer et sensibiliser pour réduire la prise sur les entreprises des fantasmes de peur véhiculés par les terroristes.

La continuité d'activité se normalise



"Normes PCA : opportunités ou obligations ?"

De gauche à droite : Lyndon Bird (BCI), Bruno Hamon (Exedis), Patrick Morrissey (Auditware) et Paul Théron (TQMS) © Journal du Net / Cécile Debise

Salle comble pour un sujet qui mobilise de plus en plus les directions d'entreprises... mais aussi les consultants. L'élaboration d'un PCA (Plan de continuité d'activité) s'impose progressivement comme une obligation, notamment d'un point de vue réglementaire et souvent en cascade, mais n'en génère pas moins des opportunités.

"La continuité d'activité est devenue un besoin vital en l'espace de 6 ans. Et les entreprises de demain se targueront de disposer d'un PCA. Cela constituera pour elles un véritable élément différenciateur dans leur relation avec leurs clients", argue Patrick Morrissey, animateur de la table et dirigeant d'Auditware.

L'ensemble des experts réunis au tour de la table, dont Lyndon Bird et Paul Théron, tous deux représentants du BCI (Business Continuity Institute), l'équivalent britannique de l'AFNOR, s'accordent en effet sur la nécessité de disposer de normes, au plan national mais aussi international, ne serait-ce que pour convenir d'une terminologie commune.

La France s'inscrit dans la continuité



"Cartographie et référentiels de bonnes pratiques"

Bruno Hamon, président du groupe de travail PCA à l'Afnor © Journal du Net / Cécile Debise

Face à l'ampleur de ce chantier que représente la continuité d'activité, disposer des bons outils et d'un référentiel paraît indispensable. C'est désormais chose faite en France, comme est venu en témoigner Bruno Hamon, en tant que président du groupe de travail à l'Afnor : Guide des bonnes pratiques pour la mise en place de plans de continuité d'activité.

Le groupe de 50 personnes de l'association française de normalisation a en effet produit en février un guide destiné à assister les entreprises dans leurs démarches. Cette plate-forme d'échange, telle que qualifiée par Bruno Hamon, pourrait déboucher sur une norme dès 2008.

Le PCA n'a toutefois pas attendu la rédaction de travaux et l'élaboration d'une norme pour se mettre en place dans les entreprises. Plusieurs secteurs, dont la banque et l'assurance, disposent en effet déjà de documents de référence, de guides de bonnes pratiques. Ces derniers ne sont cependant pas reconnus à l'international par un organisme comme l'ISO, ce vers quoi tend la BP Z74-700 de l'Afnor.

La capture de codes malveillants

[Suivante](#)



"Techniques de capture de malware"

Laurent Butti, expert en sécurité de la division R&D d'Orange © Journal du Net / Cécile Debise

Développée dans le but de nuire à un système informatique, la catégorie des *malwares* regroupe de multiples codes malveillants dont les virus, les vers, les chevaux de Troie, les backdoors et les spywares.

"Pourquoi les capturer ? Dans le but de mieux appréhender les risques et d'utiliser cette compréhension pour concevoir des modes de réaction efficaces", répond l'expert en sécurité de la division R&D d'Orange, Laurent Butti.

Cette analyse doit ainsi donner des clefs pour freiner la place croissante prise par les *bots*. Ces derniers fonctionnent en effet via un canal de contrôle par l'intermédiaire duquel le pirate donne ses instructions. Pour rendre un botnet inopérant, il faut préalablement bloquer le canal de contrôle et, pour connaître son activité réseau, il faut le disséquer, donc le capturer.

La capture se fait par le biais de pots de miel (honeypots) de moyenne interaction comme le logiciel Open Source, Nepenthes. Ce dernier peut émuler des vulnérabilités, ce qui permet d'analyser le comportement d'un binaire sur un système vulnérable. Nepenthes a ainsi été déployé sur une connexion Renater depuis fin 2005. Bilan : sur les 843 codes différents capturés, 632 sont des bots et seulement 36 des vers. 764 utilisent des techniques de protection comme les packers pour les opérations de détection.

L'argent de la malveillance



"L'argent des spywares"

François Paget, chercheur chez McAfee © Journal du Net / Cécile Debise

Depuis plusieurs années, les pirates ont amorcé le virage vers une cybercriminalité rémunératrice. Exit les défis technologiques, place à l'économie du code malveillant. Quelles méthodes utilisent les pirates et les créateurs de virus ? Quelles sommes d'argent peuvent-ils espérer récolter grâce à ces pratiques ? Des réponses avec François Paget, chercheur chez McAfee.

L'adware, programme commercial s'installant en principe avec le consentement des utilisateurs, semble assez peu rémunérateur, sauf pour un pirate disposant d'un botnet et disposé à en faire usage pour en installer. Jeanson James Ancheta a ainsi encaissé plus de 20 000 dollars pour 137 040 ordinateurs infectés par un adware. D'autres gagneraient plus de 6 000 dollars par mois.

Les codes malveillants sont également en vente sur Internet. Une backdoor peut ainsi être acquise pour un prix compris entre 200 et 400 dollars. Un prix pour lequel vous bénéficiez également d'un service après-vente... avec des mises à jour.

Du côté du spam (qui représente 91% du trafic de messages électroniques) et du phishing, la tendance est également à la hausse des bénéfices. Les 3 à 5% d'attaques par phishing fructueuses génèrent, en 2006, 1 244 dollars par victime.

Dissection d'attaques

[Suivante](#)



"Vos sites sécurisés sont vulnérables"

Jean-Marc Bost (Elca) et Olivier Busolini (NetExpert) © Journal du Net / Cécile Debise

Jean-Marc Bost et Olivier Busolini ont fait la démonstration d'une attaque de type *Man in the middle* contre un utilisateur d'un service de banque en ligne. Par le biais d'un cheval de Troie transmis via un fichier Excel piégé joint à un email, ils sont parvenus à se glisser dans la transaction réalisée par l'utilisateur.

Le code s'avère en fait être une extension intégrée au navigateur Web. Il va examiner le code de la page ouverte par l'internaute et rechercher des mots clefs pour les remplacer. Ainsi, lors d'un virement, le cheval de Troie, de manière transparente pour la banque et le client, va modifier un compte destinataire.

La démonstration date toutefois de plus d'un an, expliquent les deux experts qui, pour d'évidentes raisons de sécurité n'avaient pu faire connaître leurs travaux. Tous deux reconnaissent que, depuis, des progrès ont été faits, notamment par les banques. Si d'autres attaques ne peuvent s'appliquer, c'est avant tout du fait des limitations imposées par les sites bancaires.

Si ceux-ci souhaitent un jour étendre l'éventail d'opérations, il leur faudra passer par des solutions de sécurité empêchant les interceptions, comme l'envoi de SMS. La règle : le poste utilisateur ne peut être considéré de confiance et la solution de sécurité, tierce, ne doit pas générer un niveau de contrainte excessif.