Journal Dënschdeg, den 13. Februar 2007 – N° 030

Editorial

Prise de conscience

Tous les interlocuteurs que nous avons interrogés au cours de nos recherches pour ce dossier consacré à la sécurité informatique sont formels: utilisateurs et décideurs sont bien conscients des dangers qui guettent leurs données personnelles et de leur entreprise à l'heure du tout Internet. Les surfeurs les moins avertis auront déjà entendu parler de virus informatiques, de chevaux de Troie, de phishing ou de spam et rechigneront à fournir des données personnelles au premier demandeur. La difficulté étant évidemment de distinguer arnaque (de plus en plus professionnelle au demeurant) et demandes d'information réglementaires pour permettre une opération «business to consumer». Le meilleur arsenal de programmes «Anti»-menaces ne saurait à ce titre remplacer le principe de précaution, de mise dans toutes les opérations électroniques - le même d'ailleurs que vous appliquez lorsque vous signez un contrat quelconque...

Même contrainte évidemment pour les entreprises dans leurs transactions quotidiennes. D'autant plus qu'elles ont beaucoup plus de données sensibles à protéger (propriété intellectuelle, chiffres d'affaires, listing de clients etc.) et surtout le système informatique en lui-même, une coupure à

LuxTrust

Le gestionnaire de confiance

La naissance d'une infrastructure à clé publique n'aura pas été chose facile au Luxembourg, faute de disponibilité des infrastructures de pointe. Bien que les bases légales en étaient jetées par la loi modifiée du 14 août 2000 relative au commerce électronique, la «Public Key Infrastructure», indispensable pour la création d'une signature électronique ainsi que pour la garantie de la fiabilité tant au niveau de la sécurité que de la confidentialité et de l'inviolabilité d'une telle signature n'a vraiment démarré qu'en 2003 avec la constitution du Groupement d'Intérêt Economique LuxTrust qui institutionnalisait la coopération entre l'Etat et un groupement de banques en vue de la mise en place d'une PKI commune. En novembre 2005, l'entreprise LuxTrust S.A., détenue à hauteur de deux tiers par l'Etat luxembourgeois et la S.N.C.I. (capital social: 4,5 millions d'euros), vit le jour.

Les administrateurs-délégués, Pierre Zimmer (à g.) et Raymond Faber

Photo: F. Aussems

Timing respecté

En juillet 2006, elle se présentait au public à l'occasion de la signature d'un accord avec un consortium composé de sociétés spécialisées dans la sécurisation des données électroniques (Cetrel, Clearstream, Hitec et eBRC), déjà doté du statut de «Professionnel du Secteur Financier», statut délivré par la Commission de Surveillance du

cats SSL/TLS (Secure Socket Layer/ Transport Layer Security) au début du mois de mars et se trouve en pleine période test pour les cartes à puce permettant d'identifier les utilisateurs et de signer électroniquement.

LuxTrust», explique Pierre Zimmer, «il faut être certain à 100% à qui on a affaire. Après seulement vient l'établissement d'un certificat digital, respectivement la livraison d'une «smart card» ou d'un «token» d'identification».

Ensuite, l'intérêt pour les solu-

mais aussi et surtout de notre flexibilité», continue-t-il.

Vers un «hub» international pour le e-commerce

Les deux administrateurs-délé-

cause d'une «attaque» ou d'un sinistre pouvant évidemment compromettre le fonctionnement de l'entreprise pendant un certain temps et engendrer des pertes importantes - sans compter les effets de l'érosion de la confiance subséquente au niveau des clients.

Une étude de l'institut en sécurité informatique CSI en partenariat avec le FBI a conclu qu'une société perdait en moyenne 204.000 dollars par an consécutivement aux incidents de sécurité informatique - l'édition 2003 du rapport évaluait l'incidence des incidents même à plus de 500.000 dollars.

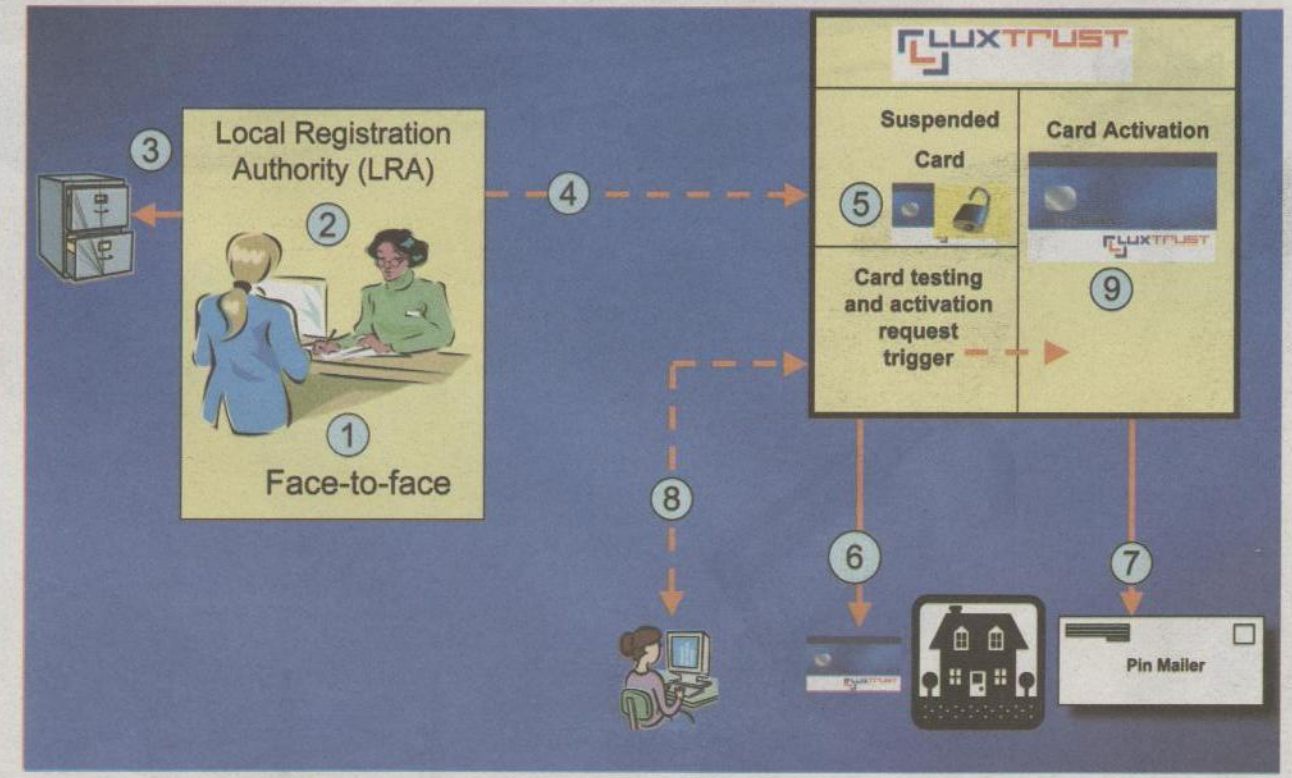
Des raisons bien tangibles dès lors pour adopter une approche pro-active dans la sécurisation des systèmes informatiques. Qui est en passe de se muter de simple «cost center» en véritable enjeu stratégique. Or, si le risque est bien compris, reste à savoir quels produit et quelle méthodologie d'évaluation et de restriction des risques mettre en place. D'après CASES, le portail de la sécurité de l'information du Ministère de l'Economie et du Commerce extérieur, des analyses récentes ont montré qu'une majorité des responsables informatiques ne sont pas capables d'évaluer le degré d'exposition aux risques de leur solution informatique et encore moins d'évaluer financièrement le risque encouru. Pour aider à la prise de décision et à la protection, www.cases.lu vaut certainement le détour, tout autant que www.clussil.lu, le site du Club de la Sécurité des Systèmes d'Information Luxembourgeois. Nous espérons que ce dossier contribuera à accélérer le processus de «prise de conscience» de l'importance de la sécurité informatique. Le «Journal» reviendra évidemment régulièrement sur la problématique. › La rédaction

Secteur Financier aux entreprises éligibles selon des critères de sécurité très sévères. Le consortium dénommé U-Trust met en place la technologie de pointe requise pour la sécurisation des signatures électroniques. Deux mois plus tard, la PKI a pris son envol et déjà passé sa première épreuve majeure avec l'introduction du passeport biométrique selon les normes internationales en août de l'année dernière.

Pierre Zimmer et Raymond Faber, les deux administrateurs-délégués se disent satisfaits de cette évolution. D'abord parce que les délais pour le «roll out» des différents projets ont pu être tenus. Comme annoncé, LuxTrust va commencer à délivrer des certifi-

Savoir à qui on a affaire

Le système des «smart cards» étant plutôt destiné à une clientèle de professionnels, LuxTrust prévoit de lancer vers la fin de l'année une solution d'identification et de signature électroniques plutôt destinée au grand public. L'utilisateur se verra remettre un porte-clé générant des codes d'accès à sa clé privée conservée sur un serveur hautement sécurisé. A défaut de porte-clé spécifique – qui change de code toutes les 30 secondes – une solution semblable pourrait être envisagée par la transmission de ce code par SMS à l'utilisateur. «Rien que l'authentification des utilisateurs représente 70% des activités de tions LuxTrust est important, selon les administrateurs-délégués. Ainsi, la plate-forme bancaire Multiline fonctionne déjà avec des produits LuxTrust, tandis que de plus en plus d'entreprises étrangères s'intéresseraient aux activités et produits de la société. «Certaines entreprises souhaitent vraiment utiliser les certificats de LuxTrust pour lancer des opérations européennes à partir du Grand-Duché», raconte Raymond Faber, en évoquant la demande d'une entreprise néo-zélandaise. «Parce que nous sommes petits, notre instrument doit pouvoir réagir à des demandes très diverses. Nous vivons bien sûr de notre infrastructure à très haut standard de sécurité,



Le processus d'enregistrement pour une «smart card»: 1. Identification du client en face à face avec un officiel de la «Registration Authority» - 2. Contrôle et enregistrement des données dans le «LuxTrust» Online Registration and Administration Tool - 3. Archivage sécurisé par un officiel de LuxTrust - 4. Transfer des données à la «LuxTrust Certification Authority» - 5. Production de la «carte intelligente» - 6. Envoi de la «smart card» au destinataire - 7. Envoi du «PinMailer» au destinataire - 8. Le client teste et active sa carte - 9. LuxTrust active la carte après en avoir été mandaté par le client

Graphique: LuxTrust

gués sont par ailleurs convaincus que le moment pour le lancement de LuxTrust a – en dépit des retards – été bien choisi. «Nous avons pu analyser nombre d'expériences à l'étranger, où certaines PKI ont vu le jour dont le concept de base était très bon, mais qui n'ont pas eu le succès escompté parce qu'elles étaient trop spécifiques à un secteur, parce que les applications pour l'utilisation pratique de leurs services faisaient défaut ou encore parce qu'il n'y avait pas d'acceptance au sein d'un public pas forcément sensibilisé aux risques de l'informatique», explique Pierre Zimmer. LuxTrust, qui fédère les efforts du privé et du public en matière de PKI – dans le développement d'applications aussi, parce qu'il existe des collaborations entre les entreprises privées et des instituts de recherche par exemple – serait en ce sens un modèle très «à la luxembourgeoise» et unique en son genre. L'objectif du Conseil d'administration, qui a élaboré un «business plan» sur cinq ans est clair: faire de LuxTrust «la» plate-forme de confiance pour le commerce et la gouvernance électroniques au Grand-Duché. En se trouvant aussi des partenaires internationaux de renom: LuxTrust vient par exemple de combiner ses propres procédures de certification à la certification Omniroot de Cybertrust, le leader mondial de la sécurité informatique pour offrir une double certification qui tourne sur presque tous les systèmes et navigateurs.

Pour atteindre ce but, l'entreprise compte aussi renforcer son marketing avec le «roll out» de ses solutions physiques d'identification. Un nouveau collaborateur a été engagé pour épauler les deux directeurs en place dans cette tâche.