Prochains sommaires

Abonnez-vous

Points de Vue

Eric d'Andigné, Elcimai : La géolocalisation au service de la sécurité bancaire

juillet 2014 par Eric d'Andigné, Directeur Général Adjoint d'Elcimai

Selon la dernière étude du Cabinet EY, ex-Ernst & Young, sondant quelque 300 banquiers européens, les priorités des banquiers français ont significativement changé. En effet, Bâle III et ses obligations de mise en conformité étaient au centre de ces priorités, alors que dorénavant la cybersécurité, citée comme importante ou très importante par 60% des sondés, tout comme l'innovation technologique (57%) qui s'y rapporte, semblent occuper toutes leurs pensées pour les prochains mois.

Comment ne pas mettre ces résultats en écho des derniers faits divers : fraude « au président » au sein d'un cabinet de conseil de renom, piratage massif d'une banque européenne qui voit 200 de ses comptes clients vidés par des cybercriminels, démantèlement par la justice américaine d'un réseau de hackers à la carte bleue,...

Chaque année, près d'une entreprise sur deux (selon PwC) est victime de fraude dont 28% de fraude liée à la cybercriminalité. En matière de fraude à la carte bleue, ce sont 3% des ménages (ONDRP) qui se disent victimes de ce type de fraude.

En France, selon l'ONDRP (Office National de Délinquance et des Réponses Pénales), le montant total de la fraude à la carte bancaire s'élevait en 2012, à 450 millions d'euros. Rien d'étonnant donc à ce que la lutte contre la cybercriminalité soit devenue la priorité des banquiers.

La mutation digitale de la Banque

Le monde bancaire n'échappe pas au vaste mouvement de transformation numérique, à la digitalisation et à la simplification des échanges et des transactions bancaires. Irrémédiablement poussés par les nouveaux usages et les attentes de leurs clients, les établissements bancaires, pour les plus avancés, proposent d'effectuer certaines actions facilement depuis leur portail internet : opérations transactionnelles, signatures d'ordres, commandes de chéquiers, gestion des ordres boursiers... Les avantages de cette nouvelle « Banque Digitale » sont nombreux : gain de temps, accessibilité 24h/24h, prise en compte des nouveaux usages, de la mobilité... Mais qu'en est-il de la sécurité associée à ces transactions ? Celles-ci sont-elles toujours aussi bien protégées que lorsqu'elles sont réalisées au guichet ? Sommes-nous réellement conscients des risques encourus ?

L'imagination des cybercriminels et des fraudeurs est sans limite

Un certain nombre de leurs cyberattaques sont connues. Parmi elles, le Phishing (et sa déclinaison sur SMS, le SMiShing), qui consiste à envoyer des mails trompeurs qui ressemblent trait pour trait à ceux de fournisseurs ou à des prestataires de services biens connus : banque, EDF, opérateur téléphonique... Ces courriels renvoient souvent à des pages où sont repris les logos et les identifiants de ces entreprises. Les victimes remplissent alors sans méfiance des questionnaires leur demandant de fournir des coordonnées bancaires. Certaines approches sont plus directes. Parmi elles, citons l'ingénierie sociale qui consiste à mettre en oeuvre des techniques de manipulations pour obtenir de sa victime des informations confidentielles (par exemple on vous demande par téléphone d'effectuer un virement prétextant des tests dans le cadre de la migration SEPA), ou encore le Pharming, technique informatique consistant à exploiter les vulnérabilités DNS en « maquillant » l'adresse IP réellement utilisée. Enfin, parmi les techniques spectaculaires, l'usurpation d'identité dite de la « fraude au président ». Dernière illustration en date, un cabinet de renom international et spécialisé dans la lutte antifraude, a récemment fait les frais de ce type d'escroquerie. Les fraudeurs, se faisant passer pour le président du groupe auprès des services financiers, ont ainsi réussi à se faire établir, au prétexte d'une opération d'acquisition confidentielle, plusieurs versements d'une valeur totale de 7.6 millions d'euros.

C'est pour toutes ces raisons que la BEFTI (Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information) renforce ses campagnes de sensibilisation à la cybercriminalité et à la cybersécurité en recommandant aux entreprises victimes de signaler tout délit informatique subit. Toutes les enquêtes menées contribuent à la prévention et à l'anticipation de ce fléau en perpétuelle évolution.

L'innovation au secours de la Banque Digitale

L'augmentation exponentielle des manoeuvres frauduleuses liées aux transactions financières fait naturellement réagir les institutions bancaires. Les impacts sont particulièrement importants et sensibles.

Au-delà même des pertes financières que la cybercriminalité peut engendrer, au-delà même de la réputation des établissements concernés et de la satisfaction de leurs clients, c'est la confiance sur laquelle l'ensemble du système repose qui est remise en cause.

Et pourtant les nouveaux usages bancaires se généralisent et les exigences d'indépendance et d'agilité des

Les événements

25 novembre 2014 : Quel avenir pour le Data Center ?

précédent

Voir tous les évènements

Vulnérabilités

- Vigil@nce - Nessus Web UI : obtention d'information
- Vigil@nce - MIT krb5 : déni de service de (...)
- Vigil@nce - Windows XP : multiples vulnérabilités
- Vigil@nce - KAuth : élévation de privilèges via (...)

All our news in english

- Vigil@nce - Nessus Web UI: information (...)
- Vigil@nce - MIT krb5: denial of service of (...)
- Abiquo and CloudSigma Partner to Deliver (...)
- Vigil@nce - Windows XP: multiple vulnerabilities

utilisateurs sont de plus en plus fortes. Faut-il pour autant considérer que le renforcement de la sécurité et la lutte contre la cybercriminalité condamnent toute innovation dans les usages de la banque de demain ?

Évidemment non, car il existe des mécanismes innovants qui concourent à la création d'une zone de confiance sécurisée avec les clients (signature électronique par empreinte digitale, géolocalisation). L'idée est de délimiter un périmètre géographique depuis lequel l'utilisateur une fois reconnu est autorisé à effectuer certaines opérations suivant une plage horaire définie par exemple. Puis selon le « device » utilisé, le contrôle des accès est réalisé soit par l'adresse IP ou par les empreintes digitales.

Autant de possibilités offertes par les innovations technologiques des différents supports (mobiles, tablettes, objets connectés) et la géolocalisation en guise de complément de sécurité aux dispositifs déjà existants.

De la sorte, la nécessaire sécurité des transactions est mieux prise en compte, sans pour autant sacrifier la volonté des utilisateurs, particuliers ou professionnels, de disposer de services à valeur ajoutée, aisément accessibles, depuis n'importe quelle plate-forme et avec le minimum de contraintes.

Les établissements financiers qui sauront proposer des services innovants, combinant ces deux contraintes, rentreront résolument dans la Banque Digitale 3.0.

Tweeter
Voir les articles suivants **Voir les articles précédents**

Actu Dossiers Vulnérabilités Malwares Agenda Guide Carrière GS Days Contact A propos Mentions légales S'identifier ADMIN