Un tournant pour la sécurité de la banque à distance ?

Sophistication croissante des attaques, esquisses de protection non intrusive du terminal client… le paysage de la sécurité de la banque à distance change. En revanche, l'espionnage de la finance par la NSA n'a pas modifié, pour l'heure du moins, les pratiques des banques.

Assurer la sécurité de la banque à distance sans imposer de smartphone au moment où les cyberattaques deviennent

La sécurité des infrastructures informatiques des banques a été sous les projecteurs de l'actualité depuis les révélations d'Edward Snowden à la presse allemande. La branche «Follow the Money» de la NSA aurait accédé aux données des transactions du réseau Visa ainsi que du réseau Swift afin d'alimenter une base de données financières de plusieurs millions d'enregistrement. Quel impact ces révélations ont-elles eu sur les pratiques de sécurité des banques françaises ? Aucun pour le moment. « Cette absence de réaction nous a fortement surpris » confie à ce sujet Renaud Bidou, directeur technique de l'éditeur français Deny All. Ces révélations ont pourtant montré clairement que certains équipements d'origine américaine comportaient des « backdoors » facilitant des écoutes indiscrètes. Pour l'heure, les banques françaises continuent de déployer certains équipements montrés du doigt. Faudra-t-il attendre que l'ANSSI intervienne pour qu'elles engagent une réflexion de fond sur ce sujet sensible ? Les mois prochains apporteront de premiers éléments de réponse. Un récent sondage du prestataire de services managés de sécurité NTT Communications auprès de mille DSI dans le monde montre en effet que les trois quarts d'entre eux vont réétudier de fond en comble les modalités de protection de leurs données.

En marge de cette péripétie, loin d'être anodine, les infrastructures réputées ultra-sécurisées des banques subissent de plus en plus d'attaques ciblées particulièrement sophistiquées. « Ce sont surtout les attaques par déni de service distribué qui inquiètent les banques pour le moment » explique Thierry Karsenti, directeur technique pour l'Europe chez CheckPoint, pionnier du firewall. Et pour cause : la disponibilité du service en ligne conditionne la confiance du client et la réputation de l'établissement. Jusque là, les banques gardaient les bases de données dans leur datacenters et déportaient le frontal de l'application Web chez un hébergeur disposant d'une large bande passante afin de résister aux attaques DDoS. Cette architecture est remise à plat depuis que les cybercriminels lancent des attaques de type « slow & low ». Ce sont des attaques de plus courte durée et de plus faible amplitude afin de ne pas être détectées de suite avant l'effondrement du service. Les cybercriminels en profitent alors pour demander des rançons. « Répondre à ce type d'attaque nécessite d'installer de nouveaux équipements sur le réseau et d'apprendre à s'en servir » précise Thierry Karsenti.

Les banques françaises ne sont plus à l'abri non plus de campagnes de phishing avec des emails écrits dans un français sans faute. « La France est moins épargnée qu'elle ne le fut à une époque » constate François Marchessaux, associé en charge du secteur bancaire chez Colombus Consulting, cabinet de conseil en stratégie et management. Près de 70 % du phishing financier visait des banques de premier plan l'an dernier, en hausse de 20 %. La France échappe de moins en moins à ces attaques. Les banques vont-elles continuer à jouer la surprotection ? Peu probable, car cette politique, adaptée à la protection périmétrique, coute cher et ne répond plus aux récentes évolutions technologiques. « Une protection plus sélective et plus dynamique, centrée sur les données, va prendre progressivement le relais » estime François Marchessaux. Il est vrai que les nouvelles attaques ciblées remettent en cause la protection périmétrique par

contrainte au client qui s'y connecte à partir de son PC ou son plus ciblées ressemble fort à la quadrature du cercle

leur niveau de sophistication. « Pour y faire face, de nombreuses banques françaises ont mis en place des équipes afin de travailler sur des projets dédiés à ce nouveau contexte » explique Loïc Guézo, évangéliste Sécurité de l'information pour l'Europe du Sud chez Trend Micro, l'un des éditeurs les plus avancés dans la détection de ce type d'attaques. « Même s'il n'y a pas eu de nouvelles familles d'attaques sur les infrastructures des banques à distance ces dernières années, leur sophistication n'a cessé de progresser » confirme Renaud Bidou. Les vecteurs d'attaque, les techniques d'évasion pour ne pas être détecté et l'impact ont connu d'importantes innovations ces deux dernières années. Ainsi, même si les attaques de Cross Site Scripting XSS datent de plus dix ans, elles deviennent plus difficiles à bloquer car elles utilisent pour vecteur du texte, de l'image ou du plug-in flash. Elles font appel à des codes non alphanumériques ou de l'encodage et servent à faire des captures d'écran ou de keylogger. Elles prennent aussi des navigateurs comme relais ou établissent des réseaux de botnets. Idem en ce qui concerne l'injection SQL ou d'autres familles d'attaques largement connues, mais que ces nouvelles sophistications rendent plus dangereuses. Quelle est la réponse des banques face à ces nouveaux phénomènes ? Les plus proactives en matière de sécurité mettent en place des solutions spécialisées. Les moins proactives se contentent de solutions généralistes moins ciblées. Ces dernières sont plus économiques et ne remettent pas en cause la formation des experts du département sécurité.

LA PROTECTION DU TERMINAL DU CLIENT RESTE UN PROBLÈME

Assurer la sécurité de la banque à distance sans imposer de contrainte au client qui s'y connecte à partir de son PC ou son smartphone au moment où les cyberattaques deviennent plus ciblées ressemble fort à la quadrature du cercle. « Les banques se cherchent encore, partagées entre la sécurité et l'expérience client, deux exigences parfois contradictoires » explique Soraya Menaï, Partner, marché banque, chez Sopra Consulting. Elle tire sa conviction d'un travail de veille permanent mené par Sopra Consulting sur la banque digitale en France et dans le monde. « La montée en charge des transactions bancaires est inexorable, mais elle nécessite de changer le mode de pensée informatique » estime pour sa part David Milot, directeur EMEA solutions du constructeur Unisys. Le problème de la sécurité du poste client est d'autant plus crucial que plus de 45 % de ceux qui gèrent leurs finances à distance sont convaincus que leur banque les remboursera en cas de vol. Tel est du moins le résultat d'une enquête réalisée par B2B International pour l'éditeur russe Kaspersky Lab. Cette croyance a de quoi surprendre à l'heure où les malwares sont capables de contourner les outils de sécurité mis en place par les banques afin de dérober de l'argent en ligne. Le danger ne vient pas que des malwares visant le terminal du client : une page Web de phishing sur quatre imite le site d'une banque ou d'un service de paiement. L'objectif reste inchangé : inciter le client à divulguer ses données bancaires. « Il n'est guère surprenant que les cybercriminels préfèrent s'attaquer aux terminaux des utilisateurs plutôt qu'à l'infrastructure informatique ultra-sécurisée des banques » remarque Tanguy de Coatpont, directeur général de Kaspersky Lab en France. La tâche du hacker est d'autant plus facile que le client ignore souvent les risques réels et néglige les mesures élémentaires de sécurité lorsqu'il se connecte. L'étude indique que 28 % des clients ne vérifient pas l'authenticité du site Web sur lequel ils saisissent leurs données confidentielles. 34 % ne prennent aucune précaution pour éviter leur interception sur les réseaux Wi-Fi publics alors que la fraude à distance est en constante progression.

Face à ce problème, les banques ont mis au point diverses techniques pour protéger le client, notamment avec l'authentification. Cependant, remarque Tanguy de Coatpont, « une protection complète ne peut être assurée que par des solutions dédiées, conçues pour répondre à la nature spécifique des cybermenaces financières ». C'est pourquoi l'éditeur a créé la plate-forme Kaspersky Fraud Prevention à destination des banques. Elle accepte les terminaux Windows, Mac, Android et iOS. Avec cette solution, le poste client est sécurisé sans intrusion puisque la plate-forme scanne sa vulnérabilité et lance un mode « secure browser » qui évite l'injection de code SQL, la copie du clavier virtuel, vérifie l'URL et les certificats et active une fonctionnalité antiphishing. La sécurité est ainsi assurée de bout en bout jusqu'au poste client. Cette approche n'est pas nouvelle : le français Deny All propose depuis deux ans un mode sécurisé sur les principaux navigateurs…mais qui n'a rencontré aucun écho commercial auprès des banques ! La plate-forme Kaspersky Lab intègre également des composants serveurs capables d'identifier les activités frauduleuses, même si le client n'a pas installé la solution de sécurité sur son équipement. « Cette solution permet aux banques de protéger leurs clients et de sauvegarder au passage leur propre réputation » précise Tanguy de Coatpont. La banque équatorienne Pichincha Bank, qui compte 750 000 clients, a déployé la solution de Kaspersky Lab. « Les banques françaises sont très intéressées par cette solution de sécurité de bout

La plupart des banques françaises tournent le dos à une comme en termes financiers. Elles se contentent du clavier d'un token. « Cet arsenal atteint ses limites » estime Thierry

en bout » affirme Tanguy de Coatpont. Ce type de solution sera-t-il adopté par les banques ? La question reste posée. « La meilleure approche serait d'installer sur le poste client un bureau virtuel qui fonctionnerait comme un sas pour accéder au site de la banque en ligne » affirme Renaud Bidou. Cette approche serait moins lourde que d'en passer par l'authentification forte. « Les banques ne veulent pas d'une authentification forte qui serait ressentie comme trop contraignante du point de vue du client » remarque Soraya Menaï, avant d'ajouter que « l'expérience client questionne en permanence les processus de sécurité et vice versa ». La plupart des banques françaises tournent le dos à une authentification forte, lourde à gérer, en termes logistiques comme en termes financiers. Elles se contentent du clavier virtuel, et pour les transactions du mot de passe SMS et parfois d'un token. « Cet arsenal atteint ses limites depuis que les hackers sont capables de compromettre le PC et le mobile d'un client » estime Thierry Karsenti. Quoiqu'il en soit, d'ici peu, « le client va être de plus en plus impliqué dans les processus de sécurité sur PC ou sur mobile, notamment depuis l'entrée en vigueur du SEPA qui desserre les montants des virements » estime François Marchessaux. Pour le moment, les banques françaises complètent leurs méthodes d'authentification par des outils de scoring qui analysent les transactions. De tels outils sont proposés par Nice Actimize ou SAP. « L'analyse du comportement client grâce à des algorithmes et des outils de modélisation est utilisée dans de nombreuses institutions financières dans le monde » confirme Jean-Michel Schneider, directeur de la filiale française récemment crée de l'éditeur américain Fico. Sa solution Falcon Fraud Manager est opérationnelle dans des établissements européens comme Deutsche Postbank, Absa Bank, Tesco Bank, EnterCard, Garanti, Swisscard et Bayern Card Services. Elle a été également implémentée chez Intesa Sanpaolo Card, institution financière italienne qui traite les transactions de onze réseaux bancaires dans le monde. Avec Falcon Fraud Manager, les pertes liées à la fraude ont été réduites de 85 % la première année au Canada et de 44 % au Brésil. L'outil a permis de centraliser les équipes qui gèrent la fraude avec une amélioration de ses analyses de 400%. Ces outils qui fonctionnent à base de règles métier analysent chaque transaction et émettent des alertes si le taux de scoring dépasse un certain seuil. En cas de suspicion, la banque peut aussi envoyer un SMS à son client pour lui demander de valider que c'est bien lui qui a réalisé telle ou telle opération. Autre possibilité : un serveur vocal appelle le client et demande de taper tel chiffre pour valider l'opération.

La conclusion est claire : l'exposition des banques à toutes ces attaques augmente à mesure qu'elles déploient le modèle digital et que les terminaux d'accès et les navigateurs se multiplient. « Conséquence, le coût de la sécurité devrait exploser si on sécurise tout de la même façon comme cela s'est fait jusque là » explique François Marchessaux. Comment alors maîtriser les coûts dans ce nouveau contexte ? Quelle sera la nouvelle structure des coûts ? Où faudra-t-il investir ? Voilà quelques unes des nouvelles questions que les banques se poseront lorsque la banque digitale sera devenue réalité. **JO COHEN**

authentification forte, lourde à gérer, en termes logistiques virtuel, et pour les transactions du mot de passe SMS et parfois Karsenti, directeur technique pour l'Europe chez CheckPoint.

La banque mobile est particulièrement visée

Sur les portails mobiles, les risques sont structurellement plus importants car la génération Y, qui vit en symbiose avec le smartphone, y est dominante. Or, selon une étude TNS Sofres commanditée par Axa Prévention, si 76 % des moins de 25 ans affirment connaître les risques du phishing et 72 % ceux de l'usurpation d'identité, 25 % d'entre eux stockent néanmoins leurs données bancaires sur leur smartphone et seulement 54 % d'entre eux verrouillent leur appareil avec un code. Pire, seulement 60 % de cette classe d'âge vérifie systématiquement ses comptes, 25 % ne le faisant que pour les grosses sommes et 13 % jamais. Le problème des malwares bancaires visant ces mobiles devient une vraie menace dans un écosystème où les banques ont peu d'expérience et où elles se contentent de répliquer les mêmes modèles de fraudes et les mêmes stratégies de prévention. « Cette menace est en très forte croissante car les appareils, les systèmes d'exploitation, les réseaux sans fil et les applications inconnues augmentent rapidement, tandis que la sécurité et la

sûreté sont souvent mises de côté car les consommateurs comme les banques n'ont qu'une idée : adopter à tout prix les paiements et les services bancaires mobiles » commente Joram Borenstein, financial crime & fraud management chez Nice Actimize. Résultat : la question de savoir qui est responsable de la sécurité, la banque, l'opérateur de mobile, le fabricant du smartphone, le développeur de l'application ou le client de la banque est toujours sans réponse. Malgré l'inquiétante croissance des chevaux de Troie bancaires visant Android et iPhone, portés par deux millions d'applications compromises, les banques restent convaincues que les portails mobiles seront à terme une source de revenus supplémentaires. Le Tower Group estime que 17 milliards de transactions se feront sur mobile dès 2015. Grand public et professionnels sont demandeurs. Reste à améliorer la sécurité des accès. « Pour l'heure, on ne peut que constater la frilosité des banques françaises en matière de fonctionnalités sur les portails mobiles » note Soraya Menai. La pression des clients risque de les obliger à forcer l'allure, le RSSI ne faisant que suivre. Aujourd'hui, jusqu'où l'accès du client à la banque mobile est-il protégé ? « Comme l'a révélé Edouard Snowden, tous les accès peuvent être contournés » rappelle David Milot, directeur EMEA Solutions d'Unisys, affirmant que « les pirates peuvent monter en marche avec des utilisateurs légitimes et atteindre de mobile en mobile les données critiques ». Les contrôles périmétriques sont ici clairement insuffisants. Unisys propose sa solution Stealth pour protéger le réseau des menaces internes en limitant le périmètre de nuisance des hackers et en confinant les attaques dans un périmètre restreint. Comme la solution Knox de Samsung, cette technique d'encapsulation des applications rend les points de terminaison invisibles pour les autres points de terminaison qui ne font pas partie de la communauté d'intérêt.