STOP

LES ATTAQUES INFORMATIQUES CONTRE LES BANQUES SONT DE PLUS EN PLUS COURANTES. ELLES SONT DANGEREUSES NON SEULEMENT POUR LES AVOIRS DES CLIENTS, MAIS AUSSI POUR LA RÉPUTATION DES ÉTABLISSEMENTS FINANCIERS. LE PROFESSEUR SOLANGE GHERNAOUTI DÉCORTIQUE CE PHÉNOMÈNE ET LIVRE QUELQUES PISTES POUR S'EN PRÉMUNIR.

PROPOS RECUEILLIS PAR NEJRA BAZDAREVIC

PROF. SOLANGE GHERNAOUTI

Directrice du Swiss Cybersecurity Advisory & Research Group
Faculté des HEC de l'Université de Lausanne
www.scarg.org

On observe une pléthore d'attaques cybercriminelles contre des institutions bancaires et financières ces douze derniers mois. D'où viennent-elles?

SG: La réalité des attaques cybercriminelles visant les institutions bancaires et financières commence à être reconnue comme un facteur de risque de déstabilisation économique et un risque réputationnel de première importance. À cela s'ajoute le problème de la fuite de données facilitée par les technologies du numérique. Il faut néanmoins rappeler que dans plus de 60% des cas connus, les pertes de données ont une origine interne et sont du fait d'employés déloyaux ayant en particulier des motivations de profit ou de vengeance.

Si l'Internet autorise une certaine proximité et facilite l'interaction entre une institution et ses clients, il favorise également la proximité criminelle et les cybernuisances. Toute communication électronique peut être potentiellement détournée à des fins malveillantes. À ce jour, il est techniquement impossible de garantir à 100% la protection ou la non-divulgation des données et la véracité des échanges.

Le risque augmente avec l'augmentation des pratiques numériques. Plus les pratiques bancaires et financières se réalisent via l'Internet, plus il y a d'ouverture et de facilité d'usage, et plus les institutions deviennent exposées. Le prix à payer de l'ouverture à Internet (sites web, réseaux sociaux, messagerie électronique, carte de paiement électronique, paiement mobile, cartes sans contact, etc.) est l'augmentation des menaces et des risques.

Doit-on s'attendre à une accélération de rythme d'assauts cybercriminels?

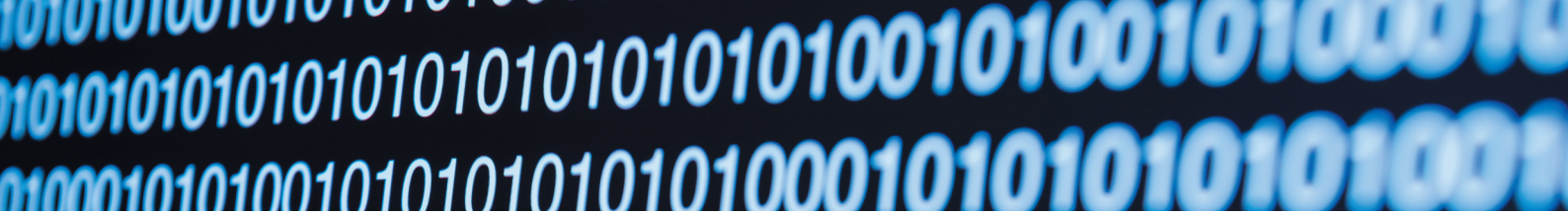
SG: Désormais, les vulnérabilités inhérentes aux technologies, dont sont devenues dépendantes les institutions, les exposent en permanence à des cybermenaces. En effet, les criminels savent exploiter toutes les vulnérabilités qui leur permettent d'optimiser leurs actions. Il peut s'agir de failles techniques liées aux codes informatiques, aux algorithmes, aux implémentations défectueuses, à des erreurs de conception, mais aussi de gestion ou d'utilisation de ces

> *« Le problème se situe au niveau du décalage entre le prise de conscience des dangers, les stratégies de gestion du risque et les mesures opérationnelles de cybersécurité mises en place. »*

technologies. Aujourd'hui, la criminalité économique est largement réalisée à distance, via l'informatique et les télécoms, notamment au travers d'Internet. Tous les indicateurs laissent penser que cela va s'intensifier dans les années à venir avec une accélération du rythme d'assauts «cyber» contre des institutions et coffres forts électroniques suisses, qui font l'objet de toutes les convoitises.

Comment ces individus peuvent-ils exploiter les données récoltées?

SG: Ce qui est plus insidieux est le fait que les escrocs profitent des outils de communication d'Internet pour être encore



aux **pirates informatiques**

plus performants. Les réseaux sociaux et les sites de rencontre sont des mines d'or pour connaître sa cible, la surveiller, monter des arnaques, leurrer des personnes et les conduire à réaliser des actions (social engineering, divulgation de droit d'accès, introduction de code malveillant…) dont les criminels tirent parti, pour s'introduire dans les systèmes informatiques, détourner des transactions ou encore par exemple réaliser des transferts de fonds à leurs avantages.

Par ailleurs, il ne faut pas perdre de vue la menace croissante émanant d'activistes ou de terroristes qui consiste à prendre le contrôle des sites web institutionnels pour revendiquer une idéologie en les défigurant et en y laissant des graffitis ou en les rendant indisponibles par des attaques en dénis de service. Une menace bien réelle, assez peu médiatisée est celle qui se traduit par la prise en otage des ressources informatiques (cryptolocking) et par une demande de rançon dont le montant semble dérisoire (de quelques centaines à milliers de francs, souvent payables en monnaie virtuelle comme le Bitcoin par exemple) au regard du pouvoir de nuisance qu'elle engendre.

Est-il possible de chiffrer les coûts engendrés par ces attaques criminelles qui préoccupent de plus en plus les banques?

SG: Il est impossible de chiffrer les impacts directs et indirects des cyberrisques ou encore d'évaluer correctement leurs effets dominos sur le long terme, car chaque situation, chaque cas de cybercriminalité sont particuliers. Les pertes de valeurs, de productivité, de confiance et d'image sont à évaluer au cas par cas. Elles peuvent cependant avoir des conséquences hautement préjudiciables pour les organisations qui en sont victimes, mais aussi pour leurs partenaires institutionnels ou clients. L'atteinte de l'une peut affecter, par effet rebond et miroir, toutes celles du secteur d'activité concerné, comme la place financière d'un pays. En fait, comme en criminalité classique, c'est la société dans son intégralité qui supporte le coût de la cybercriminalité.

Les banques ont-elles pris suffisamment conscience de ce danger et mettent-elles en place des stratégies de gestion du risque numérique solides?

SG: Le niveau de maturité des institutions dans leur prise de conscience et dans la mise en place de contremesures est fonction de leur culture et de leur histoire. Celles qui ont déjà souffert des cyberrisques ont généralement une meilleure appréciation du phénomène et savent que les impacts ne sont pas que virtuels! Il est alors plus facile de convaincre la direction générale d'investir dans la cybersécurité.

Le problème se situe au niveau du décalage entre le niveau de conscience des dangers, les stratégies de gestion du risque et les mesures opérationnelles de cybersécurité mises en place. Il peut y avoir un retard dans l'élaboration de la politique de sécurité, des insuffisances dans sa mise en œuvre, des mesures existantes, mais contournées, des procédures non respectées ou encore des processus de contrôles inadaptés

L'accès aux systèmes internes des institutions via les portables et autres supports personnels sera-t-il interdit afin de minimiser le risque d'attaques?

SG: Les technologies de l'information ont introduit de nouveaux risques dont doivent impérativement tenir compte les institutions dans leur politique de sécurité. Les stratégies de protection doivent avoir une approche réaliste qui tient compte des besoins de facilité d'emploi notamment de nomadisme, tout en assurant un niveau de sécurité adéquat. Ce sont souvent des objectifs divergents. Un compromis est à faire afin de trouver un juste milieu et une cohérence. On ne peut raisonnablement pas exiger à la fois un niveau de sécurité élevé et l'usage d'outils technologiques qui n'intègrent pas de mécanisme robuste de sécurité, cela combiné avec des comportements humains à risque. On assiste également à une sorte de fuite en avant technologique, en partie motivée par le prestige ou des tentatives d'économie budgétaire, qui, au final, met en danger les institutions et les clients.

« Les vulnérabilités inhérentes aux technologies, dont sont devenues dépendantes les institutions, les exposent en permanence à des cybermenaces. »

La FINMA a défini de nouvelles exigences en matière de protection des données des clients bancaires. Est-ce suffisant face aux menaces?

SG: Disposer de contraintes réglementaires et imposer que les institutions s'y conforment est souvent un premier pas vers une prise en compte des responsabilités et des exigences de sécurité. En revanche, la conformité réglementaire n'est pas pour autant synonyme de sécurité opérationnelle. Un des dangers est de substituer le besoin de sécurité à celui de conformité. Ceci aurait pour conséquence de dépenser beaucoup de ressources pour être en conformité et non pas pour être en sécurité et en cohérence stratégique et opérationnelle avec l'évolution des risques auxquels les institutions sont réellement confrontées au quotidien.

Comment maîtriser le risque numérique quand on est une petite entité comme le sont bien souvent les gérants de fortunes indépendants?

SG: La complexité de la sécurité du numérique et la palette de compétences nécessaires pour la maîtriser laissent le plus souvent les petites entités désarmées. Il est donc essentiel qu'elles puissent s'appuyer sur des sociétés capables de leur offrir un service intégré «clé en main» qui apporte des solutions à la fois sur les aspects techniques, managériaux, juridiques et humains; cela, tant en matière de protection et de prévention des incidents en amont, qu'en aval avec des capacités de réaction rapide et de gestion de crise. Intervenir a posteriori est fondamental non seulement pour limiter les dégâts et les réparer, mais aussi pour comprendre ce qui s'est passé, identifier les causes et les auteurs afin de mettre en place les mesures nécessaires pour que cela ne se reproduise pas. Ces mesures peuvent être des actions de formation, un accompagnement portant sur des sujets allant de l'hygiène numérique de base à la stratégie de sécurité globale incluant la cybersécurité, la contre-ingérence économique et la sécurité des installations en passant par des diagnostics de sécurité.

À qui doit-on s'adresser pour se protéger?

SG: Un véritable savoir-faire doit exister pour effectuer des investigations numériques, identifier, localiser, collecter les traces numériques, les préserver et les interpréter. Quelle que soit la finalité de l'investigation numérique — aider l'entreprise à mieux se protéger, à déposer plainte ou encore pour accompagner les instances de justice et police dans leurs missions —, l'enquêteur spécialisé en informatique forensique, doit non seulement disposer de compétences techniques pointues, mais aussi de celles qui lui permettent de présenter ses résultats de manière compréhensible par des non-techniciens. De surcroît, les dirigeants des petites et grandes institutions confondues sont exposés à des risques réputationnels consécutifs à des détournements ou vols de leurs données personnelles qui pourraient les compromettre et ainsi porter atteinte à l'image de leur organisation. C'est pour cela qu'ils doivent pouvoir également se reposer sur des compétences spécifiques, s'ils n'en disposent pas en interne, pour traiter des problématiques relatives à la gestion et à la protection de la réputation en ligne. •

La cybercriminalité en Suisse

26% d'entreprises suisses auraient subi des attaques cybercriminelles en 2014. La cybercriminalité est classée au deuxième rang de criminalité économique la plus signalée, juste après le détournement de fonds.

40% d'établissements pensent qu'ils seront victimes de cybercrime dans le futur. Cette prédiction dépasse celle qui est attendue en matière de détournement de fonds. À noter que le taux d'entreprises qui estiment qu'elles ne seront pas attaquées s'élève à 60%!

23% des participants ne sont pas en mesure de quantifier les répercussions financières des attaques cybercriminelles qui se sont réalisées. Ce chiffre témoigne du niveau de prise de conscience du danger que représente la cybercriminalité en Suisse.

Source: PWC « Global Economic Crime Survey 2014, Economic Crime: A Swiss Perspective». Une étude menée auprès d'un échantillon représentatif de l'économie suisse. Plus de la moitié des participants sont issus de l'industrie financière, manufacturière, ingénierie et construction.