STATE OF NEW YORK | EXECUTIVE CHAMBER

ANDREW M. CUOMO | GOVERNOR

Pour publication immédiate: 6 mai 2014

LE GOUVERNEUR CUOMO ANNONCE DE NOUVELLES EVALUATIONS DE CYBERSECURITE POUR LES BANQUES

Le Gouverneur Cuomo a annoncé aujourd'hui la publication d'un rapport de cybersécurité qui montre les risques croissants et la sophistication des cyber attaques que rencontrent les banques de l'Etat de New York, et a demandé au Département des Services Financiers (DFS) de mener de nouvelles évaluations régulières et ciblées de la préparation des banques que le DFS règlemente en matière de cybersécurité . Pour consulter le rapport publié aujourd'hui, cliquer ici.

« Avec la croissance des cyber menaces d'aujourd'hui, nous devons nous assurer que les finances de l'Etat de New York sont protégées contre les prédateurs en ligne », a déclaré le Gouverneur Cuomo. « Des évaluations de cyber sécurité ciblées pour les banques protègeront mieux les institutions financières contre les attaques et la violation des dossiers bancaires personnels. Lorsque les consommateurs optent pour la banque en ligne, ils s'attendent à ce que leurs informations personnelles soient sécurisées et nous nous efforçons d'assurer que les institutions financières prennent les précautions appropriées pour les protéger. »

Le Surintendant des Services Financiers, Benjamin M. Lawsky, a déclaré : « Le fait qu'autant de nos vies financières se passent en ligne fait que les banques sont des cibles de plus en plus tentantes pour les cyber-attaques. Les pirates passent des jours et des nuits à essayer de penser à de nouvelles manières de voler les informations personnelles des consommateurs, et de perturber nos marchés financiers, et il est plus important que jamais de nous mobiliser pour affronter ce défi. »

Résultats du rapport sur la cybersécurité

Sophistication croissante des attaques

Le rapport de cybersécurité publié aujourd'hui est le produit d'une enquête complète, d'un an, que le DFS a effectuée auprès de 154 banques qu'il règlemente. Le défi le plus fréquent dans l'élaboration d'un

programme de cybersécurité adapté, cité par les banques, porte sur l'augmentation de la sophistication des menaces (71%), et des technologies émergentes (53%).

La plupart des institutions ont rencontré des intrusions, ou des tentatives d'intrusion dans leurs systèmes d'information au cours des trois dernières années. Les methods utilisées pour pénétrer dans les systems d'information allaient largement, avec les institutions signalant des incidents impliquant des logiciels malicieux (malware) (22%), le phishing (hameçonnage) (21%), le détournement (7%) et les botnets ou réseaux zombies (7%).

Les types les plus fréquents d'activité illicite consécutive à une cyber intrusion rapportée par les institutions étaient les prise de contrôle des comptes (46%), le vol d'identité (18%), les perturbations de réseau de télécommunications (15%) et les violations de l'intégrité des données (9,3%). Des violations de systèmes de paiement de tierce partie ont également été rapportées par 18% et 15% d'institutions petites et grandes, respectivement. Les grandes institutions ont cité aussi l'exploitation de services bancaires mobiles (15%), le clonage sur les terminaux de paiement électronique et distributeurs de billets (23%), et les violations d'accès internes (8%).

La cybersécurité comme opportunité de développement économique

Le rapport a révélé également que la vaste majorité des banques – grandes et petites – prévoient d'accroître leurs dépenses de cybersécurité au cours des prochaines années, ce qui pourrait représenter une opportunité intéressante pour la croissance des emplois et le développement économique dans l'Etat de New York.

Plus des trois-quarts (77%) de l'ensemble des institutions ont connu une augmentation de leur budget de sécurité des informations au cours des trois dernières années, et la plupart des institutions restantes (18%) signalent que leurs budgets de sécurité des informations sont restés inchangés. Pratiquement aucune institution n'a rapporté une diminution des dépenses au cours des trois dernières années.

La vaste majorité des institutions – environ 79% de l'industrie – a rapporté que les budgets de sécurité des informations devraient augmenter au cours des trois prochaines années.

<u>De nouvelles initiatives pour lutter contre la croissance des cyber menaces</u>

Le rapport définit plusieurs mesures que le DFS mettra en oeuvre pour améliorer la cybersécurité dans les banques de l'Etat de New York. Ces mesures comprennent une nouvelle évaluation ciblée de la préparation de chaque banque à la cybersécurité – dans le cadre du processus d'examen régulier du DFS - pour contribuer à cristalliser une forte et cohérente attention sur cette question. Le processus d'examen révisé comprendra des questions supplémentaires dans les domaines de la gestion et la gouvernance des systèmes d'information, la réponse aux incidents et la gestion des évènements, les contrôles d'accès, la sécurité des réseaux, la gestion des fournisseurs, et la reprise en cas de catastrophe. Les procédures révisées visent à assurer une vue holistique de la préparation d'une

institution en matière de cybersécurité, et seront adaptées pour refléter le profil de risque unique de chaque institution. Le DFS publiera d'autres détails sur la planification et le contenu de ce processus d'examen dans les prochaines semaines.

Le DFS a également recommandé que toutes les institutions de l'Etat de New York dépositaires d'une charte, indépendamment de leur taille, deviennent membres du Centre d'analyse et de partage des informations des services financiers (Financial Services-Information Sharing and Analysis Center (FS-ISAC). Les membres reçoivent des notifications en temps opportun et des informations officielles spécialement conçues pour permettre de protéger les systèmes et biens cruciaux contre les menaces physiques et de cybersécurité. En fait, à la fois Le Département du Trésor des Etats-Unis et Le Département de la sécurité intérieure des Etats-Unis dépendent de FS-ISAC pour divulguer des informations essentielles aux services financiers en périodes de crise. De plus, FS-ISAC offre une capacité de partage d'informations de manière anonyme dans toute l'industrie des services financiers, qui permet aux institutions d'échanger des informations concernant les menaces physiques et de cybersécurité, ainsi que les vulnérabilités, les incidents, les mesures et pratiques protectives potentielles.

Le rapport d'aujourd'hui fait partie de l'engagement continu du Gouverneur Cuomo pour renforcer la cybersécurité dans l'Etat de New York. L'an dernier, le Gouverneur a créé un conseil consultatif de cybersécurité, Cyber Security Advisory Board, qui travaille avec l'administration sur des stratégies innovantes pour assurer la sécurité des New Yorkais contre les cyber menaces. La Commission a pour objectif de conseiller l'administration en matière de développement en cybersécurité et d'émettre des recommandations pour protéger les infrastructures et les systèmes informatiques cruciaux de l'État.

###

Des informations complémentaires sont disponibles à www.governor.ny.gov
État de New York | Executive Chamber | press.office@exec.ny.gov | 518.474.8418