Le vol d’identité en tête des attaques en cybercriminalité | Le Net Expert Informatique

Le vol d’identité en tête des attaques en cybercriminalité

Selon l'étude Breach Level Index pour le premier semestre 2015 publié par le leader mondial de la sécurité numérique Gemalto, il apparaît 888 failles de données signalées au cours de cette période, compromettant ainsi 246 millions d'enregistrements de données dans le monde.

Les failles de sécurité ont augmenté de 10 % par rapport au premier semestre de l'année précédente, alors que le nombre d'enregistrements de données compromis diminuait de 41 % au cours des six premiers mois. Cette nette amélioration peut être attribuée à la diminution du nombre de méga-failles à très grande échelle ayant touché le commerce de détail et la distribution, comparativement à la même période de l'année écoulée.

Malgré la diminution du nombre de données compromises, les failles les plus importantes ont touché des volumes considérables d'informations personnelles. L'incident le plus important constaté au cours du premier semestre – niveau 10 sur l'échelle de gravité du Breach Level Index –, a concerné un vol d'identité dont a été victime l'assureur-santé Anthem Insurance aux États-Unis, qui a impacté 78,8 millions de fichiers, soit le tiers (32 %) de l'ensemble des fichiers de données volés au cours du premier semestre. Parmi les autres failles notables recensées au cours de la période d'analyse, il faut citer une attaque touchant 21 millions de fichiers de l'US Office of Personnel Management (9,7 sur l'échelle BLI) ; une attaque touchant 50 millions de fichiers de la Direction générale de la population et des affaires de la citoyenneté en Turquie (9,3 sur l'échelle BLI) ; et une défaillance affectant 20 millions de fichiers du site de rencontre russe Top Face (9,2 sur l'échelle BLI). Les dix principales cyber-attaques ont représenté 81,4 % de l'ensemble des fichiers compromis.

« Nous sommes obligés de constater le fort retour sur investissement des attaques sophistiquées que mènent les hackers, qui affectent des volumes considérables de données. Les cybercriminels continuent de s'approprier, la majeure partie du temps en toute impunité, des jeux de données extrêmement précieux. A titre d'exemple, les failles qui ont touché le secteur de la santé au cours du premier semestre leur ont permis de recueillir en moyenne plus de 450 000 fichiers de données, soit une augmentation de 200 % par rapport à la même période de 2014 », explique Jason Hart, vice-président et directeur de la technologie, en charge du pôle protection des données chez Gemalto.

Incidents par source

Le nombre d'attaques conduites à l'instigation ou avec la bénédiction d'un État ou d'un service gouvernemental n'ont représenté que 2 % de l'ensemble des incidents enregistrés. Le nombre de fichiers affectés par ces épisodes représente toutefois 41 % de l'ensemble des fichiers compromis, en raison notamment de l'attaque ayant ciblé Anthem Insurance et l'US Office of Personnel Management. Alors qu'aucune des dix principales failles enregistrées au premier semestre 2014 n'était le résultat d'une action soutenue par un État, trois des principaux incidents recensés cette année ont été menés à l'instigation de services gouvernementaux et notamment les deux premiers en termes de sévérité.

Les intrusions malveillantes menées à titre individuel ont cependant été la principale cause des failles de données enregistrées au premier semestre 2015, représentant 546 ou 62 % des attaques informatiques, contre 465 ou 58 % au premier semestre de l'année écoulée. 116 millions (soit 46 %) des fichiers affectés globalement l'ont été en raison d'intrusions malveillantes, ce qui constitue un net recul sur les 298 millions d'incidents (71,8 %) répertoriés en 2014.

Incidents par type

Le vol d'identité demeure, au premier semestre, la principale cible des cybercriminels, représentant 75 % de tous les fichiers affectés, et un peu plus de la moitié (53 %) des failles de données enregistrées. Cinq des dix principales failles, y compris les trois premières – toutes trois classées au niveau « catastrophique » sur l'échelle BLI –, ont porté sur des vols d'identité, contre sept sur dix au cours du premier semestre 2014.

Incidents par secteur

De tous les domaines d'activité recensés, les secteurs gouvernementaux et de la santé ont payé le plus lourd tribut à la cybercriminalité, puisqu'ils représentent environ les deux tiers (31 % et 34 % respectivement) des fichiers de données compromis. La santé ne représente toutefois que 21 % des atteintes informatiques enregistrées cette année, contre 29 % au cours du premier semestre de l'année précédente. Le secteur du commerce de détail et de la distribution connaît une nette diminution du nombre de fichiers volés, représentant seulement 4 %, contre 38 % au cours de la même période de l'année écoulée. En termes de localisation géographique, les États-Unis sont le pays le plus touché, avec plus des trois quarts (76 %) des failles de données enregistrées, et près de la moitié (49 %) de l'ensemble des fichiers affectés par des attaques. La Turquie représente 26 % des compromissions de données, avec notamment une attaque massive ciblant la Direction générale de la population et des affaires de la citoyenneté, au cours de laquelle quelque 50 millions de fichiers numériques ont été forcés dans le cadre d'une intrusion malveillante.

Le niveau de chiffrement utilisé pour protéger les données exposées – capable de réduire considérablement le nombre et l'impact des failles de données –, a légèrement augmenté et se situe à 4 % pour toutes les attaques enregistrées, contre 1 % au cours du premier semestre 2014.

« Malgré la fluctuation du nombre de failles de données, la question reste la même : il ne s'agit pas de savoir 'si' vous allez être victime d'un vol de données, mais 'quand'. Les données collectées dans le cadre de l'étude Breach Level Index montrent que la majeure partie des sociétés ne sont pas en mesure de protéger leurs données dès lors que leur défense périmétrique a été mise à mal. Alors même qu'un nombre croissant d'entreprises procèdent à un chiffrement de leurs données, elles ne le font pas au niveau requis pour réduire l'ampleur et la gravité de ces attaques », explique Jason Hart. « Les entreprises doivent adopter une vision de la menace numérique centrée sur les données, à commencer par l'instauration de techniques de gestion des identités et de contrôle d'accès beaucoup plus efficaces, qu'il s'agisse de procédures d'authentification multifactorielle ou du chiffrement des données, pour rendre inutilisables les informations dérobées. »

Selon le cabinet Forrester, l'habileté et la sophistication croissantes des cybercriminels se traduisent par une érosion de l'efficacité des contrôles et techniques de sécurité classiques, essentiellement basées sur un contrôle périphérique. La mutation constante du paysage de la cybercriminalité nécessite donc de nouvelles mesures défensives, avec notamment la généralisation des technologies de chiffrement. Dans l'avenir, les sociétés procéderont par défaut à un chiffrement dynamique de leurs données, mais aussi lorsque leurs systèmes et leurs données seront au repos. Cette approche de la sécurité centrée sur les données s'avère beaucoup plus efficace pour lutter contre des cybercriminels déterminés. En adoptant le chiffrement des données sensibles, qui les rend inutilisables, les sociétés incitent les cybercriminels à aller chercher des cibles beaucoup moins bien protégées. Le chiffrement est appelé à devenir la clé de voûte de la sécurité informatique. Ce sera donc un élément stratégique central pour les responsables de la sécurité et de la gestion des risques au sein des entreprises.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://afriqueinside.com/securite-numerique-les-vols-didentite-en-tete-de-la-cybercriminalite09092015/