Publié le 20 octobre 2017

Protection des données et cybersécurité : les premières actions à mener

Dans un monde ouvert et numérique, la place de la gestion et de la sécurité des données est devenue incontournable. Les nouvelles règlementations et le nombre d'incidents liés à la sécurité informatique obligent dorénavant les entreprises, y compris les Epl, à s'équiper en matière de protection de leurs informations numériques. Oui mais comment ? C'est le constat de départ fait lors de la table ronde du 12 octobre autour de la Cnil, lors du Congrès de Bordeaux.

Thomas Dautien, directeur adjoint de la conformité de la Commission nationale de l'informatique et de libertés (Cnil), précise les contours de la **réforme de la protection des données**. Les obligations du nouveau règlement européen 2016/679 sur la protection des données personnelles devront être mises en place dès mai 2018 par les Epl. De nombreuses formalités auprès de la Cnil vont disparaître. En contrepartie, la responsabilité des Epl sera renforcée. Elles devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Pour se préparer, Thomas Dautieu rappelle **les 6 étapes** qu'il convient de mettre en place :

– désigner un pilote pour la gouvernance des données personnelles de l'Epl,- cartographier les traitements de données personnelles,- prioriser les actions à mener,- gérer les risques,- organiser les processus internes,- documenter la conformité.

La protection des données est à intégrer dans le processus de la sécurité informatique. En France, le nombre d'incidents liés à la sécurité informatique — tous secteurs d'activité confondus — a augmenté de 38 % entre 2015 et 2016. En 2017, 55 % des entreprises prévoient d'accroître leur budget consacré à la cyber- sécurité.

La fraude au président Natacha Schreiber, directrice marchés logement social & économie mixte, Banque du développement régional, réseau Caisse d'Epargne-Groupe BPCE appelle notre attention sur les différentes menaces auxquelles les sociétés sont confrontées.

"*Une des fraudes la plus courante est la* **"fraude au président"***, à laquelle plusieurs Epl ont été confrontées,* explique-t-elle. *L'escroquerie consiste à convaincre le collaborateur d'une société à effectuer un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre*". Souvent situés à l'étranger, les escrocs collectent en amont un maximum de renseignements sur l'entreprise notamment via le vol de données. Cette connaissance de l'entreprise associée à un ton persuasif et convaincant est la clé de réussite de l'arnaque. L'opération est alors lancée sur les personnes capables d'opérer les virements (services comptables, trésorerie, secrétariat...).

"*L'ensemble des dispositifs mis en place par le Groupe BPCE afin de sécuriser les transactions en ligne de leurs clients notamment via des mécanismes de* ***renforcement des identifiants*** *dont le certificat électronique, des habilitations sur les salariés en charge des transactions, etc.*", rappelle Natacha Schreiber.

Sécuriser, c'est établir des priorités Dans ce contexte de mise en œuvre du règlement protection des données et de sécurisation des données **Yvain Tavernier**, manager spécialisé en sécurité des systèmes d'information du cabinet **Wavestone** conseille d'identifier les menaces auxquelles les Epl doivent faire face, les grands principes et les premières leçons à retenir de la mise en œuvre du règlement et les premières actions à lancer.

En pratique, si les Epl doivent sécuriser, il sera difficile de tout traiter, il faut en conséquence établir des priorités. Il conseille :

– d'identifier et de traiter l'essentiel. Par exemple, une Epl de transport public devra concentrer son effort sur la sécurisation des SI qui permettent d'amener les passagers à destination en vie avant de sécuriser ceux qui permettent de les amener à l'heure.

– de traiter les 20 % les plus importants, à savoir les 20% des données et processus métiers les plus critiques, et les applications, réseaux, individus, sites qui supportent la production de ces données et processus.

– d'identifier et de prioriser les traitements à risques pour les personnes concernées.

Dans les premières actions à mettre en œuvre, les Epl devront :

– traiter l'existant,- établir un plan d'action et le mettre en œuvre, – contrôler l'efficacité des actions mis en place.

Philippe Labro, directeur des partenariats, direction des collectivités d'EDF rappelle l'importance des dispositifs de prévention et de sécurité qui doivent être mis en place tant dans les sociétés que dans les collectivités. "*Dans ce contexte, EDF a participé à une concertation avec l'Agence nationale pour la sécurité des systèmes d'information (Anssi) qui a abouti à un guide proposant une méthodologie simple et adaptée pour sécuriser les systèmes*", conclut-il.

Enfin, dans les conseils pratiques, il précise qu'en cas d'attaque de type cheval de Troie type Dritex,

il convient de déconnecter le réseau.

Photo (de g. à dr.) : Yvain Tavernier, Natacha Schreiber, Thomas Dautieu, Philippe Labro. ©Stéphane Laure, stlaure@gmail.com

– Réécoutez la séance en format **podcast : La cyber-sécurité, un enjeu primordial des entreprises**

– Réécoutez l'interview des intervenants au débat sur **Radio immo**

Par Marie COURROUYAN