Intelligence économique

A Roissy, 733 PC portables perdus chaque semaine

Website : https://www.sbedirect.com/grand-comptes/fr/

Environ 88 % des ordinateurs sont perdus ou volés en dehors du lieu de travail. Les cas les plus fréquents se déroulent dans les transports, en particulier les aéroports ou les gares. En effet, chaque semaine plus de 4000 ordinateurs sont oubliés ou égarés dans les aéroports européens, tandis qu'au moins un ordinateur est volé chaque jour dans les trains Thalys sur les trajets Paris-Bruxelles. Les données sont donc beaucoup vulnérables lorsqu'elles quittent l'enceinte de l'entreprise.

Vols en entreprise : quelles sanctions pour le salarié?

LE FIGARO - le 23/07/2018

Le vol par un salarié de biens de l'entreprise entraîne souvent des poursuites pour faute lourde. Mais l'employeur doit obligatoirement apporter des preuves, sous peine de voir sa sanction qualifiée d'«injustifiée».

Du stylo au gobelet de la machine à eau, le vol en entreprise reste un délit. Et les conséquences peuvent être lourdes pour le salarié. «C'est un problème important pour les entreprises», explique Éric Rocheblave, avocat spécialiste en droit du travail. «Cela peut être des biens matériels comme des biens immatériels. Les données informatiques par exemple», précise-t-il.

Les sanctions peuvent aller de l'avertissement au licenciement pour faute grave. «C'est un problème difficilement appréhendable», ajoute l'avocat. Car pour pouvoir poursuivre un salarié, l'employeur doit obligatoirement apporter une preuve des faits. «Il faut prouver que tel salarié a volé tel objet avant de le sanctionner», explique Éric Rocheblave.

Pas de recours financier pour l'entreprise

L'employeur engage des poursuites, souvent au motif de faute lourde. Mais «le vol en soit ne constitue pas une faute lourde. Pour attribuer cette sanction, il faut prouver l'intention du salarié de nuire à l'entreprise, tient à préciser l'avocat. La proportion de la sanction est ensuite appréciée par les juges en fonction de l'objet volé, de l'âge et des antécédents du salarié mis en cause», ajoute-t-il. Plus vous êtes nouveau dans l'entreprise et plus vous avez d'antécédents de ce genre, plus votre sanction pourra être dure.

«Les juges acceptent parfois des erreurs de parcours. Par exemple, pour un salarié présent depuis vingt ans dans l'entreprise sans aucun antécédent, la sanction retenue pourra être le licenciement mais sans la faute lourde», précise Éric Rocheblave. Et les preuves sont souvent difficiles à fournir. «C'est à ce moment-là que se pose la question de la vidéosurveillance. Dans quel cas peut-elle être utilisée? Jusqu'à quel point?» Et si l'employeur ne peut apporter de preuve du vol, «la sanction peut être jugée injustifiée».

Un ex-ingénieur d'Apple accusé de vol de secrets industriels

Le Parisien|11 juillet 2018

Un ancien ingénieur d'Apple est accusé d'avoir volé des secrets industriels concernant un projet de voiture autonome avant de rejoindre une start-up chinoise.

C'est une affaire aux frontières de l'espionnage industriel et des conflits de propriété intellectuelle. Apple avait embauché Xiaolang Zhang en décembre 2015 pour qu'il intègre un projet « top secret »visant à développer du matériel et des logiciels pour des véhicules autonomes. Au mois d'avril, l'ingénieur, qui a pris un congé de paternité, se rend en Chine avec sa famille.

Quelques jours plus tard, il informe la marque à la pomme qu'il veut démissionner pour vivre dans son pays d'origine : il souhaite rester auprès de sa mère malade et prévoit de travailler pour une start-up chinoise de véhicules autonomes, Xiaopeng Motors, basée à Canton.

Cette entreprise, considérée comme le « Tesla Chinois », a bénéficié du soutien d'Alibaba et de Foxconn pour 300 millions d'euros et s'apprête alors à commercialiser un premier SUV électrique ultra-connecté.

Jugeant que Zhang se montre « évasif », son supérieur chez Apple fait intervenir une équipe de sécurité. Le matériel de l'ingénieur est passé au crible : il s'avère qu'il a téléchargé de nombreuses données et des pièces confidentielles sur le design des futurs modèles de véhicules. Par ailleurs, le visionnage des caméras de sécurité révèle qu'il est ressorti avec du matériel du département où est développé ce projet.

Interrogé par le service de sécurité

A son retour chez Apple après son congé, l'ingénieur est entendu par la sécurité d'Apple. Au bout de plusieurs interrogatoires, il reconnaît avoir recopié des données sur l'ordinateur de sa femme via l'application d'échange AirDrop.

La marque à la pomme, qui a porté plainte, informe immédiatement le FBI, en charge aux Etats-Unis du contre-espionnage.
Quelques jours plus tard, le 7 juillet, Xiaolang Zhang est arrêté à l'aéroport alors qu'il tente de fuir en Chine. Il risque dix ans de prison et une amende de 213 000 euros. Après cette arrestation, Apple a averti tous les employés des risques qu'ils encouraient en divulguant des informations confidentielles.

Cette affaire rappelle le cas Levandowski. Ingénieur expert du véhicule autonome, Anthony Levandowski avait participé à la conception de la Google Car. Il avait ensuite quitté Google pour créer une start-up dédiée aux camions autonomes, Otto. En rachetant celle-ci l'an dernier pour 680 millions de dollars, Uber l'a recruté. Au final, Google a accusé Uber de fraude à la propriété intellectuelle, affirmant que son ancien salarié avait emporté 14 000 documents confidentiels à son départ.

Sous-marins DCNS - Le constructeur français victime d'une «fuite massive» de données

20 Minutes avec AFP - Publié le 24.08.2016 à 03:23

DEFENSE Cette fuite concernerait les sous-marins Scorpène, utilisés par les armées indienne, malaisienne et chilienne...
Les documents volés décriraient les systèmes de communication, de navigation et de lance-torpilles des appareils. Le constructeur naval français DCNS a été victime d'une fuite massive d'informations techniques confidentielles sur ses sous-marins Scorpène, ce qui pourrait alarmer les armées indienne, malaisienne et chilienne qui les utilisent, a affirmé le journal *The Australian* dans son édition de mercredi.

Le groupe DCNS, détenu à 62% par l'Etat français, a indiqué que «les autorités nationales de sécurité» françaises «enquêtent», sans donner plus de détails. «Cette enquête déterminera la nature exacte des documents qui ont fait l'objet de ces fuites, les préjudices éventuels pour nos clients ainsi que les responsabilités», a ajouté le groupe.

L'Australie vient d'octroyer un contrat de 34 milliards d'euros à la DCNS
Les 22.400 pages divulguées, que le quotidien australien affirme avoir consultées, détaillent les capacités de combat des Scorpène de la DCNS, conçus pour la marine indienne et dont plusieurs unités ont été achetées par la Malaisie et le Chili. Le Brésil doit lui aussi déployer ces submersibles à partir de 2018. La fuite pourrait également inquiéter l'Australie, qui a octroyé en avril un contrat de 50 milliards de dollars australiens (38 milliards de dollars US) au groupe DCNS pour concevoir et fabriquer sa prochaine génération de submersibles.
Les documents décrivent les sondes des vaisseaux, leurs systèmes de communication et de navigation, et 500 pages sont consacrées exclusivement au système de lance-torpilles, a précisé *The Australian*.

La fuite pourrait venir d'Inde
Selon le quotidien, la DCNS aurait laissé entendre que la fuite pourrait venir d'Inde plutôt que de France. Les données pourraient toutefois avoir été emportées hors de France en 2011 par un ancien officier de la marine française qui, à l'époque, était un sous-traitant de la DCNS. Les documents pourraient avoir transité par des sociétés du sud-est asiatique avant d'être finalement envoyés à une entreprise en Australie, poursuit le journal.
Le contrat des sous-marins australiens est revenu à la DCNS, mais le système de combat secret des 12 sous-marins Shortfin Barracudas est fourni par les Etats-Unis. Les submersibles australiens sont des versions réduites des Barracudas français. Le site internet de la DCNS affirme que le Scorpène est équipé de la technologie la plus pointue et la plus protégée, faisant de lui le plus létal des sous-marins conventionnels de l'histoire.

73% des entreprises sont victimes d'incidents de sécurité internes

Selon une étude conjointe [1] réalisée par Kaspersky Lab et B2B International, 73 % des entreprises ont été touchées par des incidents internes de sécurité informatique. La principale cause de fuites de données confidentielles reste les employés (42 %). À mesure que l'infrastructure informatique d'une entreprise s'étend, il en va de même pour le paysage des menaces : à nouveaux composants, nouvelles vulnérabilités. La situation est aggravée par le fait que les employés – en particulier ceux ne possédant pas de connaissances spécialisées – ne sont pas tous en mesure de suivre les évolutions rapides de l'environnement informatique. C'est ce que confirme une récente enquête, révélant que 21 % des entreprises touchées par des menaces internes ont perdu de précieuses données, avec à la clé des conséquences sur leur activité. Il est utile de préciser que l'étude recense les cas de fuites accidentelles (28 %) et intentionnelles (14 %).

Les incidents internes ne sont pas toujours des accidents
En dehors des fuites de données, les menaces internes concernent principalement la perte ou le vol des équipements mobiles des employés. 19 % des responsables interrogés reconnaissent égarer au moins une fois par an un mobile contenant certaines données de leur entreprise.

Un autre facteur important concerne les fraudes au sein du personnel. 15 % des participants à l'enquête se sont retrouvés face à des situations où certaines ressources de leur société, notamment financières, ont été utilisées par des employés à des fins personnelles. Si ce pourcentage paraît faible, les pertes causées par ces incidents sont supérieures aux dommages résultant des fuites de données confidentielles dans les grandes entreprises. Les PME perdent jusqu'à 40 000$ euros en moyenne en raison d'activités frauduleuses de leurs employés, tandis que ce chiffre dépasse 1,3 million de dollars pour les grandes entreprises.

« *Une solution de sécurité à elle seule ne suffit pas pour protéger les données d'une entreprise. Et c'est ce que confirment les résultats de cette étude* », commente Konstantin Voronkov, responsable des produits pour les postes de travail chez Kaspersky Lab. « *Les entreprises ont besoin d'une approche intégrée à plusieurs niveaux, s'appuyant sur une veille de sécurité et d'autres mesures complémentaires. Ces mesures peuvent comprendre l'utilisation de solutions spécialisées et l'instauration de règles de sécurité, portant par exemple sur une restriction des droits d'accès.* »

Kaspersky Lab recommande de ne pas négliger la question de la sécurité globale de son entreprise, car une protection fiable à plusieurs niveaux peut éviter à une entreprise des coûts supplémentaires engendrés par des incidents non seulement extérieurs mais aussi internes. En particulier, les technologies de défense contre les attaques DDoS et le phishing, de cryptage, de protection des équipements mobiles, des infrastructures virtuelles et des transactions financières, assurent toutes une sécurité ciblée et fiable pour les différents nœuds de l'infrastructure informatique d'une entreprise et pour les data centers.

En outre, la mise en place de diverses règles de sécurité ainsi que de services spécialisés d'investigation des incidents, d'évaluation indépendante de l'infrastructure informatique de l'entreprise et de formation du personnel permettra de réduire au minimum le risque présenté par ces menaces.

[1] The information security of businesses, enquête réalisée par Kaspersky Lab et B2B International en 2015 auprès de plus de 5500 spécialistes dans plus de 25 pays à travers le monde.