Condamnation d'EDF et prison ferme de salariés pour piratage informatique

Commentaire d'arrêt publié le **16/10/2019**, vu **742 fois**, Auteur : Droit de la sécurité informatique

Une enquête de piratage informatique à l'encontre de l'Agence française de lutte contre le dopage permet de révéler une affaire d'espionnage de plus grande ampleur mettant en cause l'entreprise EDF.

En 2008, les policiers de l'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) transmettent au procureur de la République de Nanterre un rapport de synthèse visant des faits d'intrusion dans le système informatique du laboratoire d'analyses de l'AFLD (Agence française de lutte contre le dopage). Deux années plus tôt, un audit commandé par l'AFLD, soupçonnant une intrusion informatique, avait révélé la présence d'un cheval de Troie au nom générique de Bifrost installé après l'ouverture d'un courrier accompagné d'une pièce jointe infectée par un virus informatique et permettant de contrôler l'ordinateur à distance.

Les investigations techniques réalisées par les enquêteurs confirment les éléments techniques déjà recueillis par l'entreprise d'audit informatique, un fichier malveillant contenant un logiciel de type *keylogger* permettant d'enregistrer et de récupérer à distance les frappes clavier. Ce programme apparaissait avoir été paramétré pour se connecter automatiquement sur deux sites (<Netzck.noip.com> et <Zipsni-ip.com>) du service de redirection américain <NO-IP.com>. Une demande d'entraide internationale adressée aux autorités américaines lors de l'enquête préliminaire permet de découvrir que les noms de domaines de ces sites avaient été déposés par le titulaire d'une adresse de messagerie <zipmq@ aol.com> se révélant ultérieurement appartenir à Alain Q. Après perquisition de son domicile et de l'ensemble de son matériel informatique, diverses pièces sont confisquées, et notamment des faits nouveaux dont le magistrat instructeur est saisi : « *1 420 documents non publics relatifs au fonctionnement de l'organisation Greenpeace étaient découverts, dont un fichier contenant des frappes clavier captées à distance en septembre 2006 concernant Yannick J., ainsi que des courriels envoyés ou reçus par des membres de l'organisation. Sur le même CD-Rom scellé 14, était découvert un fichier intitulé 2006.doc contenant de frappes clavier entre mai et juillet 2006 relatifs à un certain Frederick K. C. et où apparaissait régulièrement le mot EADS* ».

Au vu des résultats d'expertise, le hacker, qui travaillait depuis 2003 pour Thierry L., ancien fonctionnaire à la DGSE, dirigeant le cabinet d'intelligence économique qu'il avait créé, Kargus Consultants, reconnaît les faits de piratage du LNDD et de Greenpeace et, concernant l'association, oriente les investigations vers deux cadres de l'entreprise EDF. Après enquête, il est découvert un CD-Rom dans le bureau de Pierre Paul F. chez EDF et sa comparaison avec le scellé 14 permettait d'établir que les 171 fichiers présents sur le CD-Rom en possession de Pierre Paul F. avaient la même signature numérique que ceux présents parmi les 1 489 fichiers du scellé 14 découverts en possession d'Alain Q. et provenant du piratage par ce dernier de l'ordinateur du dirigeant de Greenpeace, « *afin de connaître à l'avance les actions du groupe contre EDF* ». De plus, les enquêteurs ont trouvé un contrat conclu entre Kargus Consultants et la direction Production ingénierie sécurité d'EDF branche Énergies portant sur une mission de veille stratégique « *sur les modes d'actions et les organisations des écologistes* ». Selon les termes de

ce contrat, Kargus Consultants, avec comme chef de projet Thierry L., était rémunérée à hauteur de 4 664,40 € par mois et « *s'engageait à mettre en œuvre tous les moyens intellectuels et matériels nécessaires pour assurer cette mission et Kargus Consultants ne pouvait être tenu responsable des conséquences de l'utilisation faite par EDF des résultats de la prestation exécutée* ».

Le cadre et son supérieur hiérarchique sont condamnés à une peine de 3 ans d'emprisonnement, dont 30 mois avec sursis et le second à 3 ans, dont 24 mois avec sursis, assortis d'une peine d'amende de 10 000 €. La seule défense de Pierre Paul F. consistait à dire qu'il ne connaissait pas l'origine frauduleuse du contenu de ce CD-Rom qu'il détenait matériellement, en affirmant ne jamais avoir lu ce CD-Rom mais « *au regard de la compétence reconnue de Pierre Paul F. en matière de sécurité et d'intelligence économique, de son évolution en interne chez EDF depuis plus de 20 ans, de l'importance éminemment stratégique de son poste sous la hiérarchie de Pascal D., il est inimaginable que le prévenu, ancien policier chevronné, ait pu négliger ainsi une éventuelle source de renseignements concernant la sécurité du parc nucléaire d'EDF. De la même manière, il est impossible que Pierre Paul F. ait pris seul l'initiative de rencontrer Alain Q. par l'intermédiaire de Thierry L. pour amener ce dernier à conclure un contrat avec Pascal D. qui ne pouvait évidemment être un simple contrat de veille stratégique sur sources ouvertes, assurée depuis 10 ans en interne selon les explications du représentant de la personne morale EDF* ». Et concernant son supérieur, « *la gravité des faits commis par un ancien haut gradé de l'armée faisant appel à une officine pour espionner par des moyens illégaux Yannick J. et Greenpeace justifie une peine mixte sévère. En répression il sera condamné à une peine d'emprisonnement de 3 ans dont 24 mois avec sursis et à une peine d'amende de 10 000 €* ».

L'ancien fonctionnaire de la DGSE est « *sanctionné par une peine mixte prenant en compte la gravité des faits qui lui sont reprochés, à une peine d'amende et à l'interdiction de gérer toute société pendant cinq ans ayant pour objet social la sécurité, le gardiennage et l'intelligence économique* », le Tribunal estimant qu'il a « *porté atteinte à l'État de droit, à la vie privée de ses cibles telles que Yannick J. et Frederick K. C. dans un dévoiement des valeurs républicaines* ». Les parties civiles obtiennent d'importants dommages-intérêts, 500 000 € à l'association Greenpeace, 50 000 € à son ancien dirigeant, 71 000 € à l'Association française de lutte contre le dopage et 50 000 € à l'avocat Frédéric Karel-Canoy.

Enfin, l'entreprise EDF, renvoyée en qualité de personne morale, est reconnue coupable et condamnée à 1,5 million d'euros d'amende. Le Tribunal considère que « *Pascal D. et Pierre Paul F. dans le cadre de leur mission, ont eu en quelque sorte carte blanche pour mettre en place les moyens d'assurer la sécurité du parc nucléaire dans le contexte sensible de la construction de l'EPR. Ils n'ont évidemment pas agi pour leur compte personnel mais dans l'intérêt exclusif d'EDF qui seule en a tiré bénéfice sous la forme concrète du CD-Rom frauduleux détenu dans les locaux d'EDF. Pascal D. et Pierre Paul F. ont agi pour le compte et dans l'intérêt de leur employeur* ».

Ainsi, la personne morale EDF est déclarée coupable des délits de recel et de complicité d'accès et maintien frauduleux aggravé dans un STAD au préjudice de Yannick J. et de Green peace et condamnée au paiement d'une amende de 1,5 million d'euros. L'entreprise EDF interjette appel de cette décision.