RÉUNION ACE CEE DU 4 MAI 2018
AU WAI MASSY SACLAY

Jack Chopin-Ferrier remercie les participants pour leur présence et remercie le directeur du WAI Massy Saclay d'accueillir ce petit-déjeuner de l'ACE CEE.

- **Deux jeunes sont présentés par ViTaCiTé – La Mission Locale**

- Céline Bardote Machado (BTS Notariat) recherche un poste d'employée polyvalente ou secrétaire en CDD jusqu'à fin août 2018, en attente de son intégration au sein de l'École des gardiens de la paix en septembre 2018 ;
- Yanis Hadliat (CAP horticole) recherche un emploi d'employé libre-service en CDI.

- **De la cybercriminalité à la fraude**

Véronique Le Tyrant, Dirigeante du cabinet Asset Finance Courtage et Présidente de la Commission Soutien au financement des entreprises du MEDEF Essonne, introduit le sujet de ce petit-déjeuner. Il s'agit de sensibiliser les entreprises aux attaques de la cybercriminalité, de présenter les bonnes pratiques pour lutter contre la fraude sur les informations stratégiques et d'informer sur les façons de se protéger contre la fraude et la cyberfraude par des solutions d'assurance (voir également les documents joints au présent compte-rendu).

- **Sensibilisation des entreprises à la cybercriminalité**

Deux personnes de la Division de l'anticipation et de l'analyse au sein de la Sous-direction de la lutte contre la cybercriminalité présentent l'organisation des services de lutte contre la cybercriminalité en France. Ils indiquent ce qu'est une cyberattaque et comment réagir lorsqu'on en est victime.

- L'organisation de la lutte contre la cybercriminalité au niveau institutionnel en France

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au Premier ministre, est le chef de file de cette organisation. Cette agence est au niveau gouvernemental un CERT (Computer emergency response team, ou CSIRT, Computer security incident response team), c'est-à-dire un centre de réponse à incidents qui a pour mission de gérer et traiter les alertes suite à des incidents et de prévenir des incidents de sécurité informatique. Il existe des CERT institutionnels, comme celui de l'ANSSI, et des CERT dans de grandes entreprises privées par exemple. Un site de l'ANSSI, cert-fr, recense toutes les attaques en cours en matière de sécurité des systèmes d'information. Les différents acteurs traitant de la cybercriminalité se trouvent au sein du ministère des Armées, du ministère de l'Intérieur et du ministère de l'Économie et des Finances. Il faut signaler l'existence du dispositif national d'assistance aux victimes d'actes de cyber malveillance, avec le site https://www.cybermalveillance.gouv.fr/ qui permet d'orienter et de conseiller les particuliers et les entreprises victimes de cyber malveillance.

Au sein du ministère de l'Intérieur, on trouve des instances traitant de la cybercriminalité au sein de la Préfecture de police de Paris, de la Gendarmerie (C3N), de la DGSI et de la Direction centrale de la Police judiciaire, à laquelle appartient la Sous-direction de la lutte contre la cybercriminalité (SDLC). La SDLC comprend un bureau de coordination stratégique, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), et une division chargée de l'anticipation et de l'analyse. Cette dernière comprend 18 personnes, dont deux policiers, le chef de la division et son adjoint. Le

reste du personnel est composé de contractuels, en raison de la nécessité de disposer de compétences très spécifiques. La division de l'anticipation et de l'analyse est le CERT de la PJ, c'est-à-dire qu'elle rend des services à la police ou à des partenaires privés avec lesquels des conventions sont signées (entreprises, etc.). Elle récupère des données, les traite, les analyse, fait de la prévention et échange de l'information, car c'est essentiel.

- Qu'est-ce qu'une cyberattaque pour une entreprise ?

Il s'agit d'une attaque des systèmes d'information dans un but malveillant sur tout type de matériel informatique : ordinateurs, serveurs, isolés ou en réseau, imprimantes, tablettes, téléphones... Il existe différents types d'attaques : cybercriminalité, atteinte à l'image, espionnage et sabotage.

Concernant la cybercriminalité, citons tout d'abord le phishing, technique utilisée pour obtenir des renseignements personnels dans le but d'usurper l'identité. Il faut être extrêmement vigilant et ne jamais répondre à des demandes d'actualisation de données dès lors qu'on n'est pas certain de l'identité de l'émetteur du mail. Malgré une information régulière à ce sujet, on note 10 à 15 % de réponses positives à ce phishing.

Ensuite le ransomware, qui consiste en un logiciel malveillant qui prend en otage des données personnelles sur l'ordinateur suite à une faille humaine ou informatique. Il prend la forme d'un mail qui contient un fichier compromis qui va chiffrer toutes les informations de l'ordinateur. Une rançon sera ensuite exigée pour libérer les données. Pour dépanner les entreprises victimes, le site No more ransom peut permettre d'obtenir une clef pour débloquer les données, mais cela ne fonctionne pas toujours. Le mieux est de ne pas ouvrir les mails, ni les fichiers inclus dans des mails dès lors qu'on n'est pas certain de l'identité de l'émetteur du mail. Et si l'on en est victime, il ne faut jamais payer, même si la somme semble modeste, car cela contribue à entretenir le système. En outre, il n'y a aucune garantie concernant la qualité de la clef qui sera communiquée par le rançonneur…

Enfin le cryptomining, qui consiste en un logiciel malveillant qui utilise la puissance de calcul d'un ordinateur pour miner des cryptomonnaies et être rémunéré. Cela a pour conséquence de ralentir l'ordinateur. Ces logiciels se trouvent dans des pièces jointes de mails ou sur des sites compromis. On parle beaucoup de ce type d'attaque en ce moment.

Concernant les atteintes à l'image, il faut noter les attaques DDoS (Distributed denial of service), dont l'objectif est de rendre un site inaccessible. Il existe aussi des attaques de défacement, c'est-à-dire l'effacement d'un site.

En matière d'espionnage, le but est de s'infiltrer discrètement dans le système d'information de l'organisation afin de capter le plus longtemps possible les informations pour les utiliser ou les revendre : attaque du point d'eau (par exemple copie d'un site Internet pour suivre et analyser les habitudes des utilisateurs) et spear phishing (chercher des informations sur un individu ou son entourage, en envoyant un mail en se faisant passer pour un collègue par exemple).

Enfin le sabotage consiste à rentrer dans les systèmes d'information d'une entreprise et à les rendre inopérants. Il faut insister sur l'absolue nécessité de mettre à jour les antivirus.

- Comment réagir face à une cyberattaque ?

Si, malgré les précautions prises, on est victime d'une cyberattaque, il faut contacter le service de police le plus proche pour les premières constatations, préserver soi-même les données ou faire intervenir un huissier ou un prestataire pour la préservation des données compromises afin de les transmettre pour pouvoir les faire analyser.

Les premières actions consistent à confiner et isoler les matériels infectés (débrancher les machines si elles sont en réseau), sauvegarder les données (si possible avoir un backup des

données en amont de l'attaque) et collecter tous les éléments relatifs à l'attaque. Plusieurs informations doivent être communiquées au service enquêteur : topologie, historique, observation, acquisition/duplication des systèmes touchés par l'incident avant et après sa survenance, documentation.

Porter plainte est essentiel, car c'est un des gros problèmes de la cybercriminalité : les entreprises veulent tourner la page au plus vite et négligent souvent de porter plainte (délai : 6 ans pour un délit). Il faut se rendre dans les services de la police, muni, pour une personne morale, d'une pièce d'identité (et d'un pouvoir si l'on n'est pas mandataire social), d'un extrait Kbis ou des statuts en cas d'association.

Enfin, il faut communiquer, pour limiter les éventuels effets négatifs sur l'image de l'entreprise.

- **Les bonnes pratiques pour limiter la fraude sur les informations stratégiques**

Jean-Marie Garcia, Dirigeant d'Aversus Aléa, Président de la Commission Environnement Sécurité du MEDEF Essonne, présente ce qu'il faut faire pour limiter la fraude sur les informations stratégiques.

Une entreprise victime d'un pillage d'informations stratégiques doit considérer qu'elle en est responsable, car c'est l'existence de carences internes qui a rendu possible ce pillage.

Une information importante, stratégique, est une information dont la perte ou la modification entraîne des préjudices financiers importants pour l'entreprise, directement ou indirectement. Il n'existe pas de petites informations : en effet, avec certaines parts d'informations, on peut avoir une idée précise de ce qui est important pour une entreprise. Pour limiter la fraude sur les informations stratégiques, il convient d'inverser les rôles, en étant offensif et non défensif : se demander quelles informations on aimerait obtenir chez un concurrent pour récupérer des parts de marché et en déduire ce qu'on doit protéger dans sa structure.

En termes de coût, on constate que le coût de la vulnérabilité baisse au fur et à mesure que l'on y consacre des moyens : 20 % des dépenses de sécurité permettent de résoudre 80 % des problèmes. Mais, au bout d'un moment, l'investissement en sécurité va être supérieur au coût de la vulnérabilité. Il convient donc de ne pas dépenser trop d'argent et de rechercher la meilleure efficacité.

En matière d'informations sensibles, il faut raisonner de la manière suivante :

- si l'information doit obligatoirement être rendue publique : si la protection juridique est possible et si son coût n'est pas supérieur aux gains attendus, il faut la mettre en place. Sinon, il faut consentir à la perte de l'information.

- si l'information ne doit pas être rendue publique : si la protection juridique est possible, si la durée maximale de protection est supérieure à la durée maximale d'utilisation du produit et si les frais ne sont pas supérieurs aux gains attendus et que l'on consent à ces frais, il faut mettre en place la protection juridique. Sinon, il faut protéger le secret (exemple de Coca, qui n'a jamais déposé le brevet de la composition de sa boisson pour ne pas la laisser tomber à terme dans le domaine public, et qui a décidé de la garder secrète).

Deux exemples de fraude :

- au cours d'une visite d'entreprise par une délégation, un membre de celle-ci vole des plans. Dans ce cas, la solution consiste à préparer systématiquement chaque visite d'entreprise : pour les déplacements et les stations dans l'entreprise, établir un circuit de notoriété pour que le visiteur ait l'impression d'avoir tout vu ; être vigilant pendant la visite ; après la visite, remonter les incidents et le cas échéant contacter les services de police.

- au cours d'un salon professionnel, un professionnel propose de scanner un QR code avec son smartphone afin de récupérer de la documentation, mais son objectif est malveillant (récupérer des données, etc.). En cas de participation à un salon, la solution, qu'on soit exposant ou visiteur d'ailleurs, est la suivante : avant le salon déterminer ce qu'on veut montrer ou pas ; prêter attention à ce que l'on dit lors des repas au restaurant ou à l'hôtel, car c'est souvent dans ces endroits qu'il y a des pertes d'informations ; pendant le salon, faire attention aux matériels (les solutions mécaniques, comme attacher un ordinateur portable, restent tout à fait efficaces car si quelqu'un essaie de s'en emparer, cela attirera l'attention) ; après le salon, organiser un débriefing afin de faire remonter les éventuels incidents.

- **Comment se protéger de la fraude et de la cyberfraude**

Sébastien Hager, Responsable Souscription Assurance Fraude chez Euler Hermes, indique comment se protéger de la fraude et de la cyberfraude.

La quatrième édition de l'étude menée par Euler Hermes avec la DFCG (Association nationale des directeurs financiers et de contrôle de gestion) auprès de 302 entreprises (PME et grands groupes essentiellement, quelques TPE) en février et mars 2018 montre que 7 entreprises sur 10 (contre 8 en 2016) ont été attaquées au moins une fois en 2017. Une entreprise sur 5 a subi plus de cinq tentatives. Une entreprise sur 3 a subi au moins une fraude avérée en 2017 (une sur 5 en 2016). 10 % des entreprises ont subi un préjudice moyen supérieur à 100 K€. On constate une banalisation et une professionnalisation du phishing. Moins d'entreprises sont attaquées, mais plus en sont victimes.

Les tentatives de fraudes les plus répandues sont : la fraude au faux fournisseur (faux RIB), avec 54 % – il convient à ce sujet de rappeler qu'il faut faire attention à la communication des organigrammes en externe ; 50 % de cybercriminalité (dont 20 % de ransomware) ; 43 % d'usurpations d'identité (avocats, banques…) ; 42 % de fraude au faux président (en baisse, mais remplacement par la fraude au faux avocat) ; 35 % de fraude au faux client (modification des coordonnées de livraison). Signalons qu'il est désormais très difficile de distinguer cybercriminalité et fraude, car tout passe par Internet.

Pour se protéger, il est indispensable d'analyser l'authenticité des informations fournies. Cela passe également par de la prévention : sensibilisation aux risques du service achats, du service livraisons et de l'accueil ; adaptation des contrôles internes, ce qui implique souvent de revoir l'organisation de l'entreprise (la mise en place de la RGPD va d'ailleurs aider) ; protection du système téléphonique et du système d'information. Il faut se méfier de l'urgence prétendue d'une opération (par exemple, un virement) : rien n'est urgent au point de ne pas procéder aux vérifications indispensables. Les grosses entreprises sont les plus convoitées, mais sont aussi les plus protégées. Une PME est peut-être moins visible, mais souvent plus vulnérable.

Cependant la prévention a ses limites, et la souscription d'une assurance permet de transférer le risque sur une compagnie d'assurances. Aujourd'hui, une entreprise sur deux envisage de s'assurer ou est assurée. Euler Hermes propose EH Fraud Cover, qui est une assurance-dommages pour couvrir les conséquences directes des fraudes internes (réalisées par un salarié), externes (usurpation d'identité) et cyberfraudes. Différents types de frais sont pris en charge : en cas de cyberattaque, indemnisation du prestataire qui vient débloquer le système d'information, remboursement des frais de notification – la rançon éventuellement payée n'est, elle, pas remboursée. Les frais liés aux détournements des systèmes de téléphonie sont également pris en charge, tout comme les frais de poursuites judiciaires engagés par l'entreprise et les frais de communication. Pour souscrire, il est nécessaire de compléter un questionnaire, qui est d'ailleurs un excellent moyen de

comprendre la sensibilité de son entreprise aux risques de fraude et d'évaluer les mesures prises. La prime varie en fonction du capital souscrit et de l'organisation de l'entreprise.

Pour les entreprises dont le chiffre d'affaires est inférieur à 10 millions d'euros, il existe EH Fraud reflex, qui couvre les fraudes internes, externes et les cyberfraudes. Là encore, le questionnaire à compléter est un excellent moyen pour mesurer où l'entreprise en est en termes de prévention.

En conclusion, les solutions d'assurance, si elles sont importantes, ne se substituent pas à la prévention constamment renouvelée et adaptée, car il s'agit d'une menace protéiforme qui nécessite un processus d'amélioration continue.

Question :

- Quand on est hôtelier, on travaille avec des sites, comme Expedia, etc., et l'on reçoit régulièrement des alertes nous indiquant qu'il existe un risque. On peut être victime des conséquences d'une attaque (impayé, dépôt de plainte…). Ces entreprises comme Expedia ont-elles des obligations de déclaration de ce genre d'attaque par pays ou au niveau international ?

Réponse :

- Les législations varient d'un pays à l'autre, mais les obligations en la matière se développent. Les OIV (opérateurs d'importance vitale) ont des obligations nationales, mais pas internationales. La plupart des entreprises internationales ont un CERT (voir plus haut) qui traite ce genre d'incident avec l'objectif de partager les informations.

Question :

- Il est dommage qu'on ne puisse pas porter plainte par Internet et que seule la préplainte soit enregistrable en ligne.

Réponse :

- C'est en cours, le dépôt de plainte en ligne devrait être opérationnel fin 2018 ou début 2019.

Question :

- Compte tenu du phishing lié à la recherche sur Internet, est-il judicieux d'effectuer ses recherches sur Internet sur un autre ordinateur ?

Réponse :

- Il ne faut pas confondre le phishing et les SPAMS. Mais il est certain qu'une segmentation des tâches dans l'utilisation des ordinateurs est un moyen de limiter les risques. Rappelons le site https://www.signal-spam.fr/ pour signaler les SPAMS.

- **Prochain petit-déjeuner de l'ACE CEE :**

- vendredi 1er juin 2018 à l'hôtel Best Western l'Orée. A 10 h 30, Assemblée générale de l'ACE CEE, puis déjeuner en présence des maires du territoire.