Cybersécurité et espionnage industriel

Sensibilisation aux cybermenaces, aux tentatives d'extorsions et à l'espionnage industriel dans les petites entreprises
Comment anticiper et s'en protéger à faible coût ?

Le 21 Septembre 2017 sur le campus de l'EFREI-ESIGETEL, 30-32 Avenue de la République, 94800 Villejuif

80% des entreprises françaises ont déclaré être l'objet de cyberattaques , mais les 20% restantes en sont peut être victimes, tout en l'ignorant.

Les données de votre entreprise sont un bien précieux qu'il faut protéger. Par nécessité commerciale, toute entreprise navigue aujourd'hui dans le cyberespace : connections Internet, mails, échanges d'informations via les réseaux sociaux, cloud, opérations bancaires,…
La plupart du temps, tout se passe sans problème. Mais un petit nombre de personnes mal intentionnées, les cybercriminels, scrutent constamment le cyberespace pour repérer les failles et glaner des informations stratégiques sur les entreprises ou les individus, pour perturber ou bloquer leur activité commerciale, les rançonner,… Ils opèrent souvent pour le compte d'un tiers.

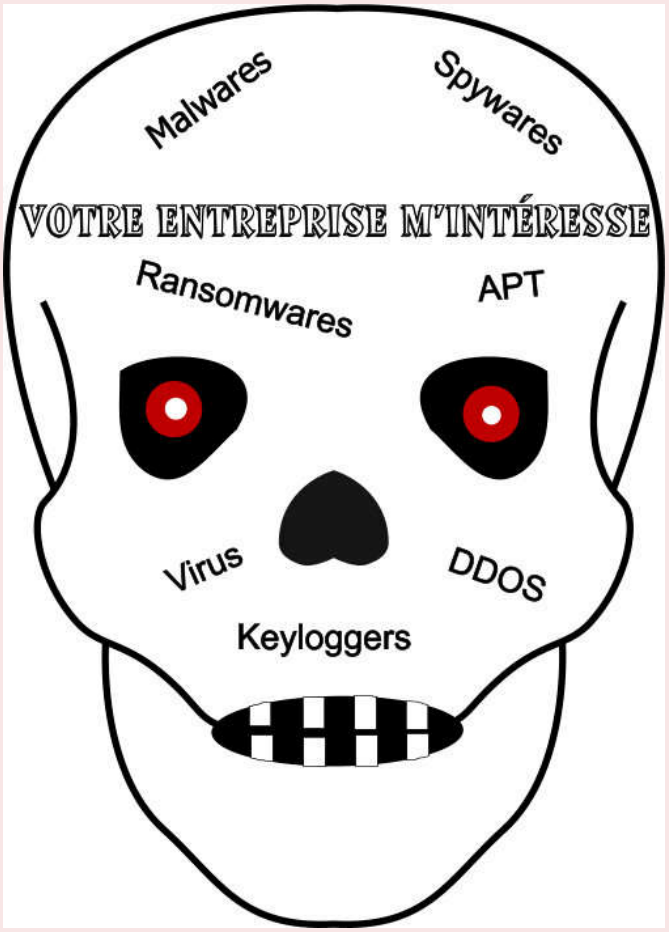
Les cybercriminels opèrent jour et nuit, souvent avec des procédures automatisées. Ils sont localisés un peu partout dans le monde et difficiles à neutraliser. Ils attaquent les grosses comme les petites entreprises. La presse se fait régulièrement l'écho des attaques menées sur de grands groupes comme Yahoo, eBay, Orange, Sony,... mais les petites entreprises sont également concernées, soit par des attaques directes, soit par les effets collatéraux d'attaques de grands groupes chez qui des données de sous-traitants ou de clients ont pu être dérobées. Les petites entreprises sont également un point d'entrée pour attaquer les grands groupes avec lesquels elles sont en relation.
Selon nos sources, près de 80% des cyberattaques concernent les petites entreprises. Ces attaques revêtent des formes diverses : la majorité concerne des « attaques éclair » localisées dans le temps, mais les APT (Advanced Persistent Threats ou menaces persistantes avancées) sont plus insidieuses : elles peuvent s'étaler sur plusieurs mois permettant aux cybercriminels d'envahir le cyberespace d'une entreprise pour siphonner ses données stratégiques.
Celle-ci ne s'aperçoit en général de l'attaque que plusieurs mois après que celle-ci ait débutée (8 mois en moyenne).
L'homme est également un point faible du système et les cybercriminels exploitent de plus en plus les failles humaines, par « l'hameçonnage » ou l'ingénierie sociale. Une bonne sensibilisation du personnel permet de réduire ces formes de risque.

Si les grandes entreprises se sont gréées d'équipes expertes pour gérer au mieux ces différentes situations, les petites entreprises sont souvent

moins préparées, par méconnaissance du sujet ou par le peu de disponibilités du personnel pouvant s'y consacrer, parfois aussi à cause des coûts induits.
Or, lorsque les cybercriminels ont conduit une attaque avec succès, les conséquences peuvent être lourdes : pertes financières, vol de titres (de propriété industrielle et autres), vol ou falsification de fichiers clients. Ceci peut induire des pertes de temps considérables... Dans les cas extrêmes, cela peut conduire l'entreprise à déposer son bilan.

L'objectif des cybercriminels est de déstabiliser l'entreprise, de lui extorquer des informations stratégiques ou de l'argent et cela entre souvent dans le cadre d'un espionnage industriel très organisé.
Pour prévenir de telles situations graves, il faut prévenir au mieux les cyberattaques et prendre des précautions simples pour les contrecarrer.
C'est le but de cette journée qui introduira le domaine de la cybersécurité et de l'espionnage industriel, pour des cadres et dirigeants de petites entreprises sans expertise particulière en informatique.

L'objectif est de donner une vue d'ensemble du problème, grâce à une approche simple mais complète, pour pouvoir mettre en œuvre et maîtriser une politique de protection générale des données de l'entreprise face aux cyberattaques et à l'espionnage industriel.
Des exemples concrets seront présentés, illustrant les divers scénarios possibles et les bonnes pratiques à suivre pour réduire au maximum les risques.



Programme

8H30 Accueil et café

9H Présentation de la journée et des participants (C.Ngô)

9H15-10H30 Ministère de l'intérieur

Protection des données sensibles à l'ère du numérique

10H30-10H45 Pause

10H45-12H15 Bruno Jouniaux

Espionnage industriel et menaces cyberindustrielles

12H15-13H45 Déjeuner

13H45-14H30 Michel Richard

Cybercriminalité : aspects juridiques

14H30-15H30 Christian Ngô

Cybermenaces : prévention, détection et protection

15H30-15H45 Pause

15H45-17H15 Christian Ngô (suite)

17H15-17H30 Synthèse

Après cette journée, le participant :

- Connaîtra les principales menaces
- Pourra identifier les premiers signes d'une attaque
- Pourra mettre en place de bonnes pratiques permettant de les éviter
- Pourra développer une culture de cybersécurité dans l'entreprise
- Pourra prévenir les tentatives d'espionnage industriel
- Connaîtra des adresses de sociétés permettant de résoudre des problèmes graves en cas d'attaque réussie de l'entreprise
- Sera armé pour aller au delà de ce qui a été présenté dans cette journée de sensibilisation

Dès cette première journée de sensibilisation, un **Club « Cybersécurité et espionnage industriel »** sera ouvert pour partager connaissances, expériences et documents sur ce sujet qui va prendre une place de plus en plus importante dans la vie des entreprises.

Cette journée de sensibilisation à l'espionnage industriel et à la cybersécurité est organisée par

L'association ARMIR (Association Rayonnement Mesure Industrie Recherche) favorise et développe les coopérations entre les milieux de la recherche, de l'industrie et des PME, par l'échange de connaissances scientifiques et techniques à l'échelle nationale et européenne.

www.armir.fr

Société qui intervient dans les domaines de l'énergie, des nano-technologies, de la prospective, de l'aide à l'innovation et de l'édition sous forme de conseils, de conférences et études.

www.edmonium.fr

Le groupe EFREI regroupe deux écoles d'ingénieurs associatives privées (l'EFREI et l'ESIGETEL) formant des ingénieurs dans le domaine du numérique.

www.groupe-efrei.fr

Comité d'organisation

Jean Bourliaud

Responsable de la thématique sécurité d'ARMIR. Expert en nucléaire de défense et non prolifération. Ancien conseiller du CEA auprès du ministère de l'intérieur.

Henri Camus

Membre d'ARMIR. Conseiller scientifique au CEA. Expert en nucléaire de défense, désarmement, lutte contre la prolifération et environnement.

Roger Ceschi

Directeur général de l'ESIGETEL, A été le directeur général des écoles d'ingénieur suivantes : ENSEA, ESIEE d'Amiens et ESME. Expert en traitement du signal. Auteur d'un théorème et de plusieurs ouvrages.

Bruno Jouniaux

Ancien chargé de mission cyberdéfense au CEA. Expert en nucléaire de défense. Soutien actif à la réserve cybercitoyenne (RCC).

Jacques Lefebvre

Vice-président d'ARMIR. Conseiller scientifique au CEA. Expert en nucléaire de défense, valorisation de la recherche et sécurité.

Christian Ngô

Gérant de la SARL EDMONIUM. Ancien directeur scientifique après du Haut Commissaire à l'énergie atomique et de la direction de la recherche technologique du CEA. Ancien Délégué Général d'ECRIN (Echange et Coordination Recherche-Industrie).

Michel Richard

Membre d'ARMIR. Conseiller Scientifique au CEA. Expertise scientifique et technologique, aspects juridiques et techniques de la vérification et contrôle en sécurité globale.

Les intervenants

Ministère de l'intérieur

Intervenant du Ministère de l'intérieur travaillant sur ce sujet

Bruno Jouniaux

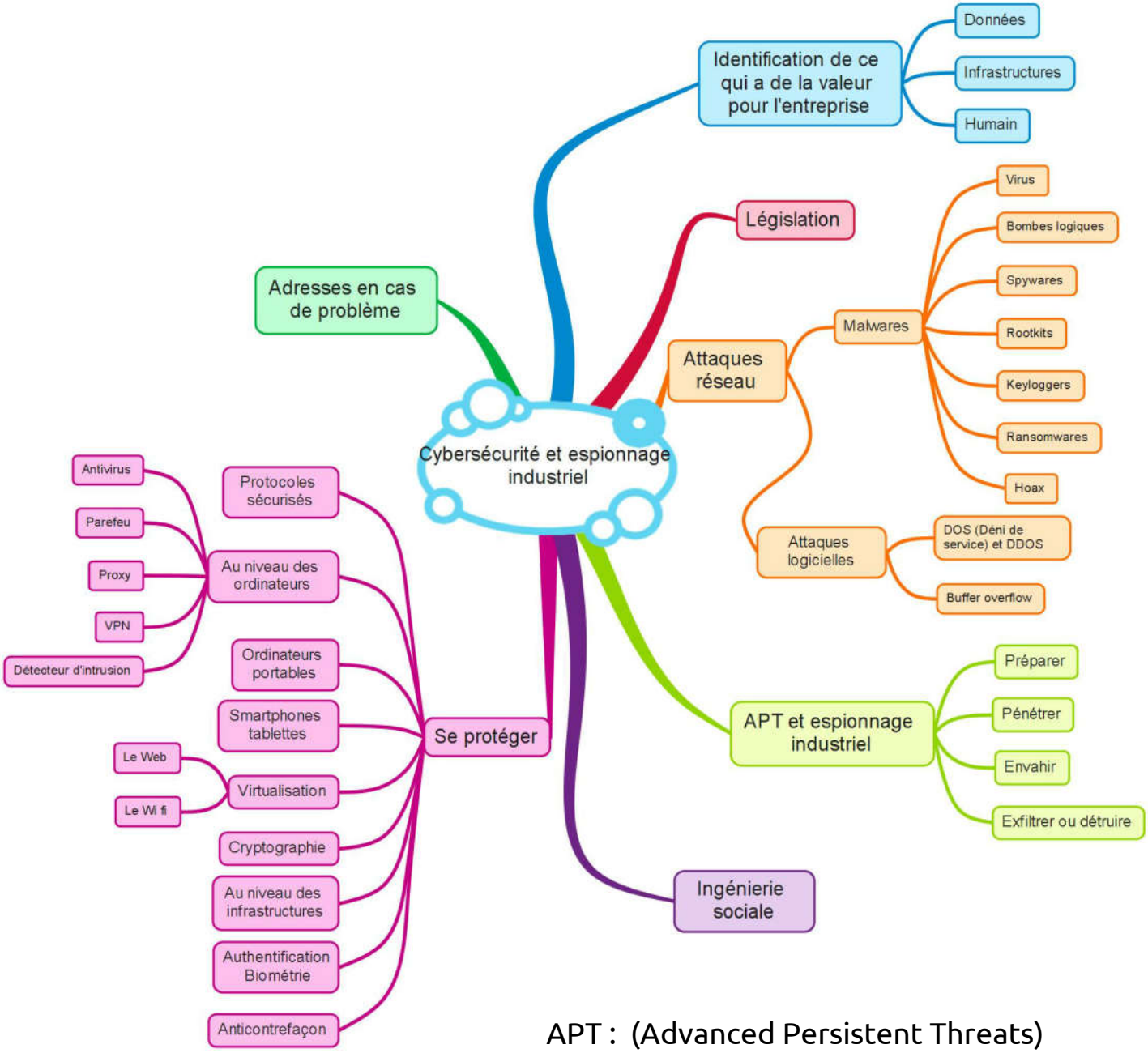
Ancien chargé de mission cyberdéfense au CEA. Expert en nucléaire de défense. Soutien actif à la réserve cybercitoyenne (RCC).

Christian Ngô

Dirigeant d'EDMONIUM. Auteur ou coauteur de plus d'une douzaine d'ouvrages dans différents domaines scientifiques. Plus de 200 publications en vingt ans de recherche fondamentale et 3 brevets en recherche appliquée.

Michel Richard

Conseiller Scientifique au CEA. Expertise scientifique et technologique, aspects juridiques et techniques de la vérification et contrôle en sécurité globale (relations internationales et européennes, non-prolifération, désarmement, traités, accords, nucléaire civil et de défense, NRBC),



APT : (Advanced Persistent Threats)

DDOS : Distributed Deni of Service

Cybersécurité et espionnage industriel

Le jeudi 21 Septembre 2017 de 8H30 à 17H30 sur le campus de l'EFREI-ESIGETEL, 30-32 Avenue de la République, 94800 Villejuif

Tarifs de participation à la journée et au déjeuner

1 personne

600 € HT soit 720 € TTC

Personne supplémentaire de la même entreprise

300 € HT soit 360 € TTC

Pour toute inscription avant le 1er juillet 2017

500 € HT soit 600 € TTC

Pour une personne supplémentaire

250 € HT soit 300 € TTC

Afin de favoriser les échanges entre les participants, la journée sera limitée à une douzaine de personnes

Cybersécurité et espionnage industriel

Le 21 Septembre 2017 sur le campus de l'EFREI-ESIGETEL, 30-32 Avenue de la République, 94800 Villejuif

Bulletin d'inscription

Nom : ……..

Prénom : ……

Société : ……..

Adresse : ……

……

Fonction : ……

Mail : ……

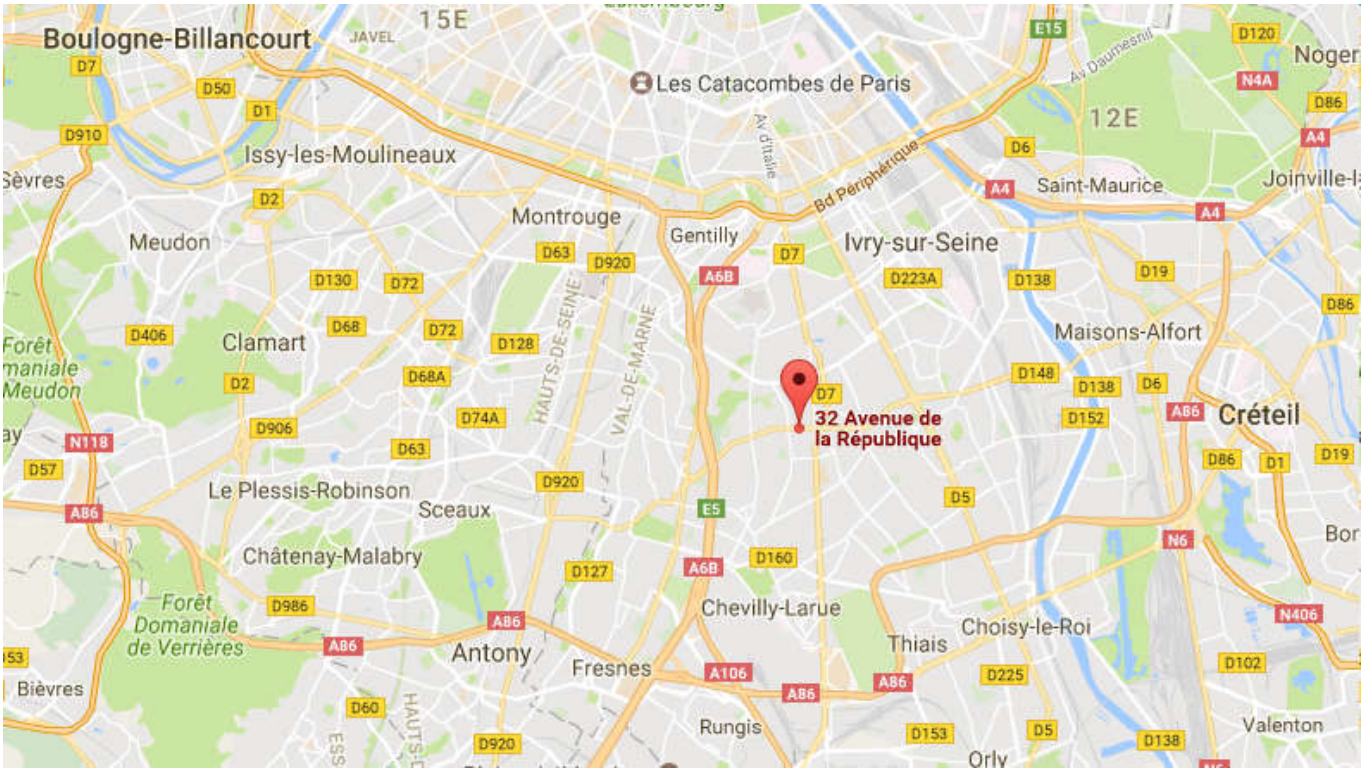
Portable : ……

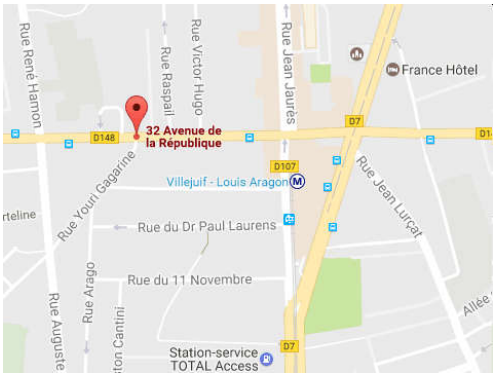
Fixe : ……

À envoyer par mail à edmonium@gmail.com

Contact : Christian NGÔ => 06 85 52 70 89

Comment venir sur le campus de l'EFREI et de l'ESIGETEL ?





Le campus de l'Efrei est situé à Villejuif, 30-32 Avenue de la république, est à 3 minutes de la station de métro : Villejuif – Louis Aragon (ligne 7).

Bus vers des stations RER : 286 (Antony), 580 (Laplace), 285 (Juvisy), 162 (Meudon-Val Fleury et 293 (Sucy en Brie)

L'aéroport d'Orly est à 15 mn en navette