# REUNION D'INFORMATION

## Compte-rendu

### Mardi 27 mars 2018

## INFOS CLUBS

**Jeudi 26 avril mars à 18h30**

*Salle de l'Orangerie à Is sur Tille*

Réunion d'information sur les réformes du Code du Travail animée par la DIRECCTE dans le cadre du Relais Conseils RH

**FORMATIONS SST RECYCLAGE ET INCENDIE**

**Jeudi 31 mai :**
Recyclage SST
*Reste 6 places*

**Jeudi 7 juin :**
Formation incendie

**Pour vous inscrire, contacter notre secrétariat**

Une réunion d'information sur le thème de la cybercriminalité, animée par l'Adjudant-Chef Franck POPILLE, Enquêteur Nouvelles Technologies au sein de la Cellule Identification Criminelle et Numérique de la Gendarmerie Bourgogne Franche-Comté, a été organisée par le Club Entreprendre et s'est tenue à la salle des fêtes de Savigny-le-Sec.

Une vingtaine de chefs d'entreprise et d'élus étaient présents à cette occasion.

A l'issue de la réunion, les discussions se sont poursuivies autour d'un verre de l'amitié offert par la municipalité de Savigny-le-Sec.

CLUB ENTREPRENDRE
ZAC Rue Les Plantes Bonjour – 21260 SELONGEY
Tel : 03.80.85.50.60 - Fax : 03.80.75.72.72
asicre@clubentreprendre21.fr – www.clubentreprendre21.fr

## LA CYBERCRIMINALITE en quelques chiffres

La cybercriminalité représente au niveau national, 5700 plaintes/mois déposées auprès de la Gendarmerie dont :
- 80% escroqueries
- 10% d'atteintes à la personne
- 10% d'atteintes aux Systèmes de Traitement Automatisé des Données (STAD).

La durée moyenne entre la compromission et la détection de l'intrusion est de 469 jours en Europe et en Afrique contre 146 jours aux Etats-Unis.

Pour endiguer ce nouveau fléau, la Gendarmerie compte :
- 60 experts criminalité numérique au niveau national,
- 260 gendarmes spécialisés dans le numérique au niveau départemental,
- 3000 correspondantes nouvelles technologies qui sont les 1ers interlocuteurs en cas de dépôts de plainte au niveau local.

Les formations de ces personnels spécialisés se font en interne et d'ici à 2022 leur nombre devrait quasiment doubler.

## PAR QUELS MOYENS ?

### *1. Les Equipements informatiques*

Indispensables aujourd'hui dans la vie professionnelle, les équipements informatiques, tels que les ordinateurs, les clés USB, les disques durs, … servent également dans la vie privée et sont souvent les mêmes. Or, il est fortement recommandé de dissocier les appareils selon leur usage et de cloisonner leur utilisation afin de ne pas propager d'éventuels virus ou se faire pirater toutes les données.

### *2. Les réseaux sociaux*

Très largement utilisés, les réseaux sociaux (Facebook, Twitter, Linkedin…) favorisent la liberté d'expression et la visibilité. Néanmoins, cela peut-être à double tranchant car les commentaires peuvent être aussi bien positifs que négatifs et l'entreprise n'aura aucune emprise sur ce qui sera publié par des tiers.

De plus, les informations qui seront mises en ligne constituent une source de données ouverte à laquelle les escrocs auront accès. Par exemple, un chef d'entreprise qui annonce qu'il part en vacances à l'étranger et que son entreprise sera fermée à telle date a potentiellement plus de risques de se faire cambrioler.

Il faut également savoir que toute image ou information publiée sur les réseaux ne nous appartient plus. Si vous publiez une image sur Facebook, elle peut être utilisée à d'autres fins que celle initialement prévue sans que vous ne puissiez-vous y opposer.

Dans ce cas également, il est fortement recommandé de dissocier les comptes personnels des comptes professionnels.

### *3. Le Cloud*

Le **cloud** consiste à exploiter la puissance de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet.
Vanté pour ces nombreux avantages : prestations clé en main, gain de productivité, possibilité de stockage, il soulève néanmoins beaucoup de problèmes concernant la sécurisation des données.
En effet, il devient difficile pour les entreprises ayant un cloud de savoir avec certitude comment et où sont stockées les données physiquement (Est-ce un serveur ? Est-il situé en France ou à l'étranger ?), ce qui va poser un réel problème au regard des nouvelles mesures européennes qui vont être mises en place en 2018 concernant la protection des données.

De plus, il est de plus en plus attaqué car il permet de récupérer le maximum de données. Cependant, les entreprises n'en ont pas forcément connaissance, leur fournisseur ne leur rendant pas de compte vis-à-vis des mesures mises en place pour sécuriser les serveurs.

### *4. Le Wifi*

Le Wifi permet une connexion sans fil aux réseaux et équipe maintenant tous nos outils numériques (ordinateur, GPS, Téléphone portable, …) afin de nous offrir plus de mobilité, un accès simplifié et rapide.
C'est avec la même facilité et simplicité que n'importe qui peut se connecter sur votre réseau, consulter et détourner vos données.

Il est à éviter le plus possible au niveau professionnel, sinon voici quelques petits conseils à appliquer:
- Cacher le SSID
- Filtrer les adresses Mac
- Utilisation de cartes wi-fi avec clef WPA2
- Pare-feu assurant des fonctions VPN voire de détecteur d'intrusion
- Identifier les utilisateurs connectés
- Limiter le niveau d'accès des utilisateurs
- S'assurer que tous les périphériques sont sécurisés.

## LES TYPES D'ATTAQUES

### 1. *Le hameçonnage*

Cette technique, aussi appelée phishing ou filoutage, est utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.
Elle consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, …) afin de lui soutirer des renseignements personnels tels que ses mots de passe, numéros de carte de crédit, numéro ou photocopie de la carte nationale d'identité, .... Une fois ces informations recueillies, l'escroc pourra pénétrer dans le système piraté et l'utiliser.

L'attaque peut être très ciblée si le fraudeur la prépare grâce aux données qu'il aura récoltées sur Internet et les réseaux sociaux.
Elle peut aussi bien être réalisée par courrier électronique que par un site internet frauduleux.

Il est important de prévenir les autorités en cas d'attaques car même si les plaintes n'aboutissent pas, les informations récoltées pourront permettre de constituer des dossiers et à terme peut-être démanteler certains réseaux.

### 2. *Les attaques virales ciblées*

Après une surveillance des habitudes de navigation de la victime ou l'obtention de données suite à un sondage frauduleux, l'escroc va lancer une attaque virale qui se propagera à l'ensemble du parc informatique de la société.
Cette pratique a pour but par exemple de réaliser un espionnage financier, espionnage industriel,…

### 3. *Les Rançongiciels*

Ces attaques, venant principalement de l'étranger, consistent en l'envoi d'une campagne de mails avec des pièces jointes malicieuses ou des liens sur des sites malveillants. Une fois la pièce jointe ouverte, l'escroc pourra crypter vos fichiers (doc, xls, odf, PDF, …) se trouvant sur vos aux disques durs, disques partagés sur les réseaux, clés USB et parfois à certains fichiers synchronisés dans le cloud et vous enverra une demande de « rançon » pour les récupérer.
Vous devrez le rémunérer en « bitcoin », une monnaie virtuelle utilisée sur Internet, en échange d'une clé de décryptage qu'il vous enverra ou pas !

Les bons gestes pour éviter cela :
- Toujours vérifier la concordance entre le nom de l'expéditeur et l'adresse mail
- Ne jamais ouvrir une pièce jointe ou cliquer sur un lien en cas de doute
- Réaliser des sauvegardes régulières de ces documents sur un disque externe
- Ne pas répondre à la demande de rançon.

Il existe un site de référence concernant ces pratiques qui nous vous invitons à consulter : www.nomoreransom.org/fr/index.html

### *4. Les défacements*

Généralement le fait d'hacktivistes pour des motifs politiques ou idéologiques ou à des fins de défi technique (challenge entre attaquants), le but de cette attaque est la modification ou l'ajout d'informations sur une page Web voir de son remplacement.

L'attaque est souvent due à l'exploitation de failles de sécurités connues et documentées.

### *5. Le deni de service ou DDOS*

Il s'agit d'une attaque spécifique qui vise à planter un système en lui envoyant une somme importante de requêtes, puis à récupérer les données quand le système est hors-service.

Le site Internet NORSE retrace les différentes attaques au niveau mondial.

### *6. Les Faux Ordres de virements*

Ce type d'attaque est moins courant aujourd'hui du fait d'une vigilance accrue.

L'escroc étudie l'entreprise afin de déterminer son mode de fonctionnement, ses habitudes en terme de fournisseurs, de clients, de montants des transactions afin d'agir de la façon la plus similaire et cohérente pour ne pas éveiller les soupçons.

Si toutefois vous répondiez à un faux ordre de virement, vous devrez contacter au plus vite votre banque avant que les transactions soient faites sur des comptes à l'étranger car il n'y a plus de recours possible après.

### *7. La fraude aux PABX/IPBX*

Cette pratique consiste au piratage de votre central téléphonique ou de votre box et laisse libre accès à votre attaquant de les utiliser ce qui peut entrainer pour la victime :
- une surfacturation des abonnements téléphoniques (appels à l'étranger ou sur des numéros spéciaux),
- l'enregistrement illicite de conversations,
- le sabotage, …

Ce qu'il est important de retenir, c'est que le facteur de l'humain est à l'origine de toutes ces attaques.

## LES BONNES PRATIQUES

Voici quelques conseils pour éviter de se retrouver confronté à une cyberattaque :

- Sensibiliser les utilisateurs et dirigeants face à la menace dont ils ne perçoivent pas les risques (Démonstrations, jeux de rôles, débriefings d'incidents…)
- Mettre à jour régulièrement ses systèmes et ses applications, dont les sites Web
- Changer régulièrement ses mots de passe en évitant les dates de naissance, noms des proches, nom de l'entreprise, …

Il est nécessaire de les complexifier en mettant le plus de caractères possibles et il existe des outils de gestions prévus à cet effet.

- Limiter les droits d'accès aux outils informatiques (ordinateur, clés USB, …), réseaux (Wifi, Internet, …), …
- Mettre en place une surveillance des systèmes d'informations (analyse des journaux réseaux et de sécurité).
- Cloisonner les systèmes afin d'éviter la propagation d'une attaque au sein des réseaux et cloisonner l'utilisation des outils informatiques en fonction des différents usages (personnels et professionnels)
- Réaliser des sauvegardes quotidiennes si possible sur un support externe stocké dans un autre lieu permettant aussi la conservation des données en cas d'incendie, de vol …
- Utiliser des alias pour les adresses mails et les différencier selon leur usage
- Détruire systématiquement les disques durs d'ordinateur, clés USB, cartes SD ou tous espaces de stockage de données avant de les jeter
- Faire attention sur l'utilisation des nouveaux objets connectés (montres, électroménagers, voitures, compteurs électriques, …)
- Utiliser le moteur de recherche QWANT plutôt que Google

**Secrétariat du Club**
Albane SICRE
Tel : 03.80.85.50.60
asicre@clubentreprendre21.fr
www.clubentreprendre21.fr