CYBERCRIMINALITE ET PROPECTION DES DONNEES A CARACTERE PERSONNEL

Ambroise Dj. ZINSOU

SECRETAIRE GENERAL DE LA CNIL BENIN

CAMPAGNE DE SENSIBILISATION

13 avril, 2017

UAC

Plan de présentation

I. CYBERCRINALITE

II. CYBERCRIMINALITE ET LES RESEAUX SOCIAUX

III.L'INTERNET DES OBJETS, LE PARADIS DES PIRATES

IV. CONSEILS

I. CYBERCRINALITE

- Le développement des TIC et la vulgarisation d'Internet ont provoqué des bouleversements majeurs,(communication à l'échelle mondiale, droit applicable).

- Emergence de nouveaux modes de communication, de nouveaux modes d'échanges,(ecommerce)

- Possibilité de transaction à distance
- Ce nouveau mode présente une nouvelle menace : la cybercriminalité

I. CYBERCRINALITE

1.1. Qu'est ce que c'est cybercriminalité ?

- Pas de définition universelle admise ,
- Chaque Etat l'a défini selon ses propres critères
- La cybercriminalité est une notion polymorphe qui peut concerner les infractions classiques commises par le biais des TIC, comme de nouvelles infractions, nées de l'essence même des TIC
- Comme la criminalité traditionnelle, elle peut prendre diverses formes et se produire à tout moment et n'importe où

CYBERCRINALITE ET PROTECTION DES DONNEES PERSONNELLES

- Les cybercriminels utilisent un certain nombre de méthodes, en fonction de leurs compétences et de leurs objectifs.

- La cybercriminalité est un type de criminalité, perpétrée à l'aide d'un ordinateur ou dans le cyberespace. Les définitions varie d'un organisme à un autre.

CYBERCRIMINALITE

- La convention sur la cybercriminalité du Conseil de l'Europe utilise le terme "cybercriminalité" pour faire référence aux délits liés à toute activité criminelle portant atteinte aux données, au non-respect des droits d'auteur [Krone, 2005].

- Zeviar-Geese, (1997-98) suggèrent d'y inclure des activités telles que la fraude en ligne, l'accès non autorisé, la pédopornographie, et le harcèlement dans le cyberespace.

- Les Nations Unies (1995), dans sa définition inclut la fraude, la contrefaçon et l'accès non autorisé .

CYBERCRIMINALITE

- Symantec s'inspire des nombreuses définitions de la cybercriminalité et donne la définition concise suivante : ***tout acte criminel perpétré à l'aide d'un ordinateur ou sur un réseau, ou à l'aide de matériel informatique***.

- L'ordinateur ou le matériel peuvent être l'agent de l'acte criminel, son facilitateur, ou sa cible. L'acte criminel peut se produire sur l'ordinateur uniquement ou à d'autres emplacements

CYBERCRIMINALITE

- également. L'étendue de la cybercriminalité est davantage compréhensible si on la divise en deux catégories, nommées cybercriminalité de type I et de type II.

  i) Cybercriminalité de type I

- Il s'agit généralement d'un événement ponctuel du point de vue de la victime. Par exemple, une victime télécharge sans le savoir un cheval de Troie qui installe un programme d'enregistrement des frappes clavier sur sa machine ;

CYBERCRIMINALITE

. Reception d’ un courrier électronique contenant un lien prétendu légitime alors qu'il s'agit en réalité d'un lien vers un site Web hostile

- logiciels criminels (les programmes d'enregistrement de frappes clavier, les virus, les rootkits ou les chevaux de Troie)

- Les failles ou les vulnérabilités d'un logiciel (des criminels contrôlant un site Web profite d'une vulnérabilité d'un navigateur Web pour attaquer la evictime (cheval de Troie)

CYBERCRIMINALITE

- Exemples de cybercriminalité de type1 : phishing, vol ou manipulation de données ou de services par piratage ou par le biais de virus, usurpation d'identité, fraude bancaire et du commerce électronique
- **ii) cybercriminalité de type II,**
- harcèlement sur Internet, prédation contre les enfants, extorsion de fonds, le chantage, la manipulation des marchés boursiers, l'espionnage industriel de haut niveau, ainsi que la planification ou l'exécution d'activités terroristes

CYBERCRIMINALITE

- La cybercriminalité de type II présente les caractéristiques suivantes :
- Il s'agit généralement d'une série continue d'événements impliquant des interactions répétées avec la cible contactée par une personne dans un forum de discussion. Petit à petit, cette personne tente d'établir une relation avec la cible. Le criminel finit par exploiter cette relation dans le but de perpétrer un acte criminel.

CYBERCRIMINALITE

- Des membres d'une cellule terroriste ou d'une organisation criminelle pourraient également communiquer sur un forum de discussion de façon codée et, par exemple, planifier des activités ou débattre du blanchiment de leur gain malhonête :
- Elle est rendu possible par des programmes qui *ne font pas partie* de la catégorie des logiciels criminels. Par exemple, les conversations pourraient avoir lieu par le biais de clients de messagerie instantanée ou des fichiers pourraient être échangés via FTP

CYBERCRIMINALITE

1.2. Cybercriminalité une menace

- Aujourd'hui, cette menace se fait de plus en plus insidieuse. Elle devient un risque majeur, en particulier pour des acteurs dont les réseaux sont susceptibles de contenir des informations monnayables, comme les entreprises ou les Etats, qui présentent l'avantage de fournir des blocs entiers d'informations potentielles, contrairement au piratage d'entités individuelles
- ..

CYBERCRIMINALITE

En effet, la cybercriminalité, à l'origine conçue comme une succession de défis à la sécurité des réseaux, qualifiée de *proof-of-concept* a pris une coloration mafieuse, donnant naissance à de véritables « marchés noirs » d'informations piratées, allant des atteintes à la propriété intellectuelle et artistique au vol d'identité, en passant par les fraudes à la carte bancaire et la violation de la vie privée

CYBERCRIMINALITE

1.2.1. Les enjeux de la protection des données pour les entreprises

- le ecommerce et les transactions effectuées en lignes, sont sujettes à de nombreux fléaux.

- Deux menaces parmi les risques encourus par les entreprises seront examinées. le hameçonnage est tout d'abord une usurpation de l'entreprise . Ensuite, l'entreprise est particulièrement touchée par le vol de ses données.

CYBERCRIMINALITE

i) Le hameçonnage, une forme d'usurpation d'identité d'entreprise

- La contrefaçon, ou l'usage d'un nom de domaine semblable à une entreprise sont des techniques qui portent atteinte à sa propriété intellectuelle. Cependant, l'internet et la multiplication des transactions en ligne a amené les cybercriminels à développer une nouvelle technique pour usurper l'identité de l'entreprise : le hameçonnage.

CYBERCRIMINALITE

Le hameçonnage, traduit de l'anglais *phishing*, désigne métaphoriquement le procédé criminel de vol d'identité par courriel. Il s'agit d'« aller à la pêche de renseignements personnels dans un étang d'utilisateurs Internet sans méfiance* »

- lIl est défini ainsi qu'il :

«***Envoi massif d'un faux courriel, apparemment authentique, utilisant l'identité d'une institution financière ou d'un site commercial connu, dans lequel on demande aux destinataires, sous différents prétextes, de mettre à jour***

CYBERCRIMINALITE

leurs coordonnées bancaires ou personnelles, en cliquant sur un lien menant vers un faux site Web, copie conforme du site de l'institution ou de l'entreprise, où le pirate récupère ces informations, dans le but de les utiliser pour détourner des fonds à son avantage »

La plupart des entreprises touchées par le hameçonnage sont les institutions financières. En effet, les escrocs convoitent particulièrement les informations bancaires, afin de détourner des fonds

CYBERCRIMINALITE

Dans ces conditions la confiance des consommateurs en ligne s'érode si aucune mesure n'est prise. Cette perte de confiance pourrait être atténuée par « la sensibilisation du grand public à la cybercriminalité, à l'usurpation d'identité, et à la violation de la vie privée ».

ii) Le vol d'informations sensibles

- Au-delà du risque constitué par l'usurpation de leur identité, les entreprises sont particulièrement vulnérables à travers leur interface Internet à plusieurs niveaux

CYBERCRIMINALITE

- En effet, plusieurs de leurs données peuvent faire l'objet d'attaques, principalement dans une perspective de vol . Parmi les données les plus sensibles selon nous, se trouvent les données techniques relatives aux innovations de l'entreprise, et les données à caractère personnel des clients, qui ont fournir leur numéro de carte bancaire lors d'une opération de commerce en ligne.

CYBERCRIMINALITE

- . l'exemple récent de l'opérateur de télécommunications américain AT&T, victime du piratage des données de près de 19000 clients notamment leurs informations bancaires, ou encore le piratage historique de plus de 40 millions de numéros de cartes bancaires Visa et Mastercard en 2005, grâce à l'exploitation d'une faille système chez le sous-traitant en charge du traitement des transactions entre les banques et les clients, *Cardsystems*.

CYBERCRIMINALITE

- L'exploitation de telles données est lucrativement très intéressante pour les pirates, qui peuvent soit s'en servir eux-mêmes pour commettre des fraudes à la carte bancaire, soit les revendre sur les réseaux *underground*

1.2.2. Les enjeux de la protection des données pour les Etats

Les Etats sont aujourd'hui de plus en plus confrontés à la cybercriminalité, d'abord de par leur rôle de protection des citoyens,

CYBERCRIMINALITE

mais surtout parce que le développement TIC les a menés à développer des sites web afin de garantir une meilleure accessibilité, et une économie de temps et d'argent substantielle à leur population. Le revers de la médaille réside en ce que certaines données personnelles relatives aux citoyens et résidents, deviennent plus facilement accessibles, en particulier sur les serveurs gouvernementaux . Par ailleurs une nouvelle menace se développe pour les Etats : le cyber-terrorisme

CYBERCRIMINALITE

i) La lutte contre le piratage des données personnelles

La protection des données personnelles est assurée par plusieurs lois dans un certain nombre d'Etats dont le Bénin. Celles-ci définissent les données à caractère personnel comme « **tout renseignement qui concerne une personne physique et qui permet de l'identifier** ». Elles posent comme principe tant pour la collecte,

CYBERCRIMINALITE

la communication et l'utilisation des renseignements personnels, le consentement préalable de la personne concernée, principe qui tombe toutefois face à certains impératifs, comme l'intérêt public ou l'avantage certain de la personne sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Les lois prévoient des sanctions contre tout contrevenant

CYBERCRIMINALITE

- Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès .

- Le non-respect de ces dispositions par celui qui traite les données personnelles, entreprise commerciale du secteur privé comme organisme public

CYBERCRIMINALITE

- est sanctionné par une autorité administrative indépendante, par exemple la CNIL, et peut aller du simple avertissement à la sanction pécuniaire, en passant par la mise en demeure et l'injonction de cesser le traitement des données personnelles
- Les sites les plus « à risque » sont ceux qui abritent les pages relatives à l'administration électronique, *et ceux* relatifs à tous les services administratifs et auxquels les usagers ont un accès en ligne

CYBERCRIMINALITE

- . Les téléprocédures, permettant aux individus de suivre l'avancement de diverses procédures administratives, de payer leurs impôts en ligne ou de procéder à des demandes d'actes d'état civil
- Enfin, pour contrer au maximum l'insécurité résiduelle d'un réseau susceptible de contenir des informations à risque, il est essentiel de mettre en place des politiques de prévention et de bonne conduite au niveau des utilisateurs du réseau.

CYBERCRIMINALITE

- En effet, malgré une sécurisation efficace du réseau, bien souvent on se rend compte que la faille est humaine. Il est recommandé à cette fin l'emploi de mesures de sécurité, tant physiques (claviers verrouillés, utilisation de câbles antivols pour les ordinateurs portables), que technologiques (utilisation de mots de passe, documents chiffrés) ou administratives (accès restreint aux renseignements).

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- L'espionnage informatique peut se déguiser sous des masques très subtils, et notamment sous la forme des fameux « cookies »

- au-delà de cet enjeu de sécurisation des données personnelles dites « sensibles », les Etats connaissent d'autres menaces dont l'importance ne cesse de croître, parmi lesquelles le cyber-terrorisme

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- ou des requêtes que vous effectuez sur les moteurs de recherche. Si ce n'est généralement pas de l'espionnage malveillant avec des préjudices moraux ou financiers pour l'internaute, ces méthodes peuvent porter atteinte à la vie privée où nous tromper sur les prestations réelles d'une société.
  - Méthodes utilisées

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- L'IP tracking; consiste à pister l'adresse IP de l'internaute et ses moindres fréquentations sur internet à des fin marchand l'objectif étant de réaliser son profil. Il l'inonde ensuite de publicité. Cette pratique en soi est légale tant que le fournisseur ne trompe pas le client
- LES COOKIES
- Au nombre des méthode de l'IP tracking utilisées sur les forums, y compris les réseaux sociaux, et dans le e-commerce,

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- on peut citer les COOKIES qui ont pour mission de :
- sauvegarder vos préférences lorsque vous surfez régulièrement sur un même site (langue, mise en page, etc) ;

- sauvegarder les paramètres de vos applications et des plug-ins associés (version, etc) ;

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- sauvergarder les paramètres des pages web consultées (feuilles de style, javascripts, date de connexion, sécurité en place, etc) ;

- sauvegarder les paramètres sur votre localisation (adresse IP publique, pays d'origine, ville, etc) ;

- sauvegarder votre pseudonyme (login) et/ou votre mot de passe, etc ;

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- A chaque connexion que vous faites sur un site, s'il n'y a aucune restriction définie dans votre programme ou votre navigateur, le site concerné pourra lire et mettre à jour ces cookies. Cela permet notamment :
- lors d'une connexion sur un site sur lequel vous vous êtes déjà connecté, d'ouvrir votre session automatiquement sans devoir encoder votre pseudonyme ni votre mot de passe et en tenant compte de vos préférences ;

2. **CYBERCRIMINALITE ET LES RESEAUX SOCIAUX**

- tant qu'une connexion à Internet est établie et sans devoir vous connecter sur aucun site, de vous informer en tout temps de la disponibilité d'une nouvelle version (mise à jour) d'un logiciel que vous avez installé ;

- le vendeur du site consulté peut affiner votre profil d'internaute afin de dresser votre profil d'achat et vous proposer des publicités ciblées pendant que vous surfer sur son site.

Les OTT

- **Les OTT**

- **GOOGLE et FACEBOOK**

- Google en 2010 a avoué qu'il espionnait les liaisons Wi-Fi dans le cadre du projet "Street View". Les employés de Google stockent les informations privées récoltées sur votre ordinateur et les communiquent le cas échéant à la justice.

Les OTT

- Si Microsoft et Facebook font de même ainsi que la plupart des opérateurs afin d'écarter leur responsabilité dans les affaires de cybercriminalité, cela signifie aussi que ces sites ont les moyens de récolter des informations privées et donc pas uniquement celles qui sont publiques.
- les cookies que nous avons décrits ci-dessus sont utilisés par la plupart sinon tous les sites Internet. Google utilise également l'IP tracking pour extraire, conserver et analyser les centres d'intérêts des internautes

4. L'INTERNET DES OBJETS, LE PARADIS DES PIRATES

- Après les réseaux sociaux, "l'Internet des objets" prend de plus en plus d'importance : moyennant une mini caméra ou un émetteur GPS, grâce au réseau cellulaire ou Internet, il est possible en permanence de vous localiser

.aujourd'hui les nouveaux modèles de voiture, d'ordinateur, de TV, de frigo, d'APN, demain notre cuisinière, notre radio digitales seront reliés à Internet et communiqueront avec le service après-vente du fabricant

4. L'INTERNET DES OBJETS, LE PARADIS DES PIRATES

- Selon une étude du cabinet Gartner, en 2009 il y avait 2.5 milliards d'objets connectés dans le monde. En 2013, on en dénombrait 9 milliards et il y aura plus de 30 milliards d'objets connectés vers 2020 dont 10 milliards de mobiles .

- Un tel parc informatique est une mine d'or pour les hackers

5. CONSEILS

- Installer un anti-virus authentique et à jour sur votre ordinateur pour prévenir toute attaque;

Supprimer tout lien entre les sociétés et notamment Google et votre ordinateur après chaque consultation en supprimant les cookies de votre ordinateur ;

- supprimer les historiques de votre navigateur Internet y compris les cookies, mots de passe et autres traces

CONSEIL

- . En effet, en supprimant les cookies, le site marchand n'ayant plus accès à l'historique ni au profil de l'internaute, il ne pouvait plus établir de lien entre l'ordinateur et les produits consultés

- activer l'option "navigation privée". Dans ce cas également, aucune information (historique, cookies, fichiers temporaire) n'est sauvegardée sur votre ordinateur. Seuls les fichiers téléchargés seront sauvegardés

Conseils

- débrancher votre modem ou votre routeur afin qu'il obtienne une nouvelle adresse IP.

Cette solution ne doit être utilisée qu'en cas de problème technique également configurer votre messagerie pour bloquer tous les courriers indésirables mais cette solution est lente et pas très efficace.

Conseil

- Une autre solution consiste à installer un firewall (pare-feu) à la place de votre modem ou un firewall software sur votre ordinateur

- installer une messagerie associée à un mot de passe et d'autres stratégies de protection. Tout ce que vous envoyez ou recevez comme courrier électronique doit être authentifié sinon ils sont refusés

Conseil

- Le logiciel anti-virus, anti-spyware, anti-spam, la messagerie sécurisée et le firewall sont des solutions très efficaces qui vous mettront à l'abri de pratiquement tous les actes cybercriminels
- éviter d'afficher votre adresse e-mail sur Internet, même cachée derrière le bouton d'un script, car toute personne malveillante pourra facilement la recopier sur un forum.

Conseils

- Le logiciel anti-virus, anti-spyware, anti-spam, la messagerie sécurisée et le firewall sont des solutions très efficaces qui vous protégeront contre tout acte cybercriminel

- Eviter d'afficher votre adresse e-mail sur Internet, même cachée derrière le bouton d'un script, car toute personne malveillante pourra facilement la recopier sur un forum.

Conseils

- Pour éviter ces problèmes, sur les forums et les sites de ventes en ligne, la plupart des utilisateurs ont trouvé une parade : ils utilisent une adresse e-mail publique (par exemple sur le domaine de gmail ou outlook) qui peut éventuellement recevoir du spam et du courrier indésirable qu'il suffira de supprimer

- Se méfier des inconnus qui vous proposent des cadeaux

Conseils

- Faire ses propres recherches;
- En cas de doute, jouer la carte de la prudence;
- Interdire les mauvaises annonces (et les mauvais annonceurs)
- Éviter l'usurpation d'identité

CYBERCRIMINALITE

- **MER**CI POUR VOTRE ATTENTION