

L'ABC des bonnes pratiques pour se protéger des Cyberattaques | Denis JACOPINI



Pour se prémunir des cyberattaques, la meilleure solution consiste à mettre en place quelques bonnes pratiques de base.

Encourager une gestion rigoureuse des mots de passe

Mettez en place des outils qui forcent les utilisateurs à choisir des mots de passe forts. Ceux-ci comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des symboles du clavier (!, @, \$, etc.), mais aucun mot entier. Ils doivent aussi être changés régulièrement, même si ça cause de la grogne.

Sensibiliser les employés

Souvent considérés comme la porte d'entrée des cybercriminels, les employés doivent être formés, par exemple au moyen de modules d'apprentissage vidéo, sur les risques d'attaques possibles et les différentes formes qu'elles peuvent prendre.

Effectuer régulièrement des tests

Une façon de vérifier si les campagnes de sensibilisation auprès des employés fonctionnent consiste à les tester en simulant, par exemple, l'envoi d'un courriel frauduleux. N'oubliez pas de l'envoyer aussi – et même surtout – à ceux qui occupent des postes stratégiques.

Limiter l'accès à l'information confidentielle

Ne donnez accès aux renseignements confidentiels qu'à ceux qui en ont réellement besoin dans l'entreprise.

Contrôler les processus de sécurité

Rien ne sert d'avoir des systèmes informatiques à la fine pointe si on ne les teste pas régulièrement. Il vaut mieux impartir la tâche à des experts si on ne possède pas les ressources nécessaires à l'interne. Les fournisseurs de solutions infonuagiques disposent d'une infrastructure de sécurité informatique qui peut bien souvent dépasser celle des entreprises.

Installer les mises à jour logicielles rapidement

Beaucoup d'attaques exploitent des vulnérabilités connues depuis plusieurs mois par les fournisseurs d'antivirus, qui d'ailleurs offrent déjà des correctifs pour les contrer. Prévoyez l'installation des mises à jour dans un délai optimal de 48 heures, ou d'au plus une semaine.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <https://www.lesaffaires.com/classements/les-500/cyberattaques-l-abc-des-bonnes-pratiques/579150>

Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications | Denis JACOPINI

Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications

Maintenant que la Loi Renseignement est votée, et en attendant la suite du processus législatif, apprenons à résister à la surveillance de masse avec quelques outils cryptographiques plus ou moins simples, mais efficaces et légaux.

Nous sommes le soir du mardi 5 mai, et c'est un jour funeste pour la démocratie. La France s'était autoproclamée « pays des Lumières » parce qu'il y a 250 ans notre pays éclairait l'Europe et le monde grâce aux travaux philosophiques et politiques de Montesquieu, qui prônait la séparation des pouvoirs, et de Voltaire et Rousseau. À dater d'aujourd'hui, jour du vote en première lecture du projet de loi sur le renseignement, à cause d'une classe politique d'une grande médiocrité, s'enclenche un processus au terme duquel le peuple français va probablement devoir subir une loi dangereuse, qui pourrait s'avérer extrêmement liberticide si elle tombait entre de mauvaises mains, par exemple celles de l'extrême droite.

Même si la loi doit encore passer devant le Sénat puis peut-être revenir en seconde lecture à l'Assemblée Nationale, même si une saisine du Conseil Constitutionnel va être déposée par une soixantaine de courageux députés en complément de celle déjà annoncée par François Hollande, mieux vaut se préparer au pire, en imaginant que cette loi sera un jour promulguée. En faisant un peu de mauvais esprit, j'ai imaginé un nom pour le dispositif qui sera chargé de collecter nos données personnelles afin de détecter les comportements suspects : « Surveillance Totale Automatisée via des Systèmes Informatiques » et bizarrement l'acronyme est STASI !

Dès lors, à titre préventif et sans préjuger de l'avenir, il me semble important d'apprendre à protéger sa vie privée. Ceci passe par le chiffrement de ses communications, qu'il s'agisse d'échanges sur Internet ou via SMS, et cela peut se faire au moyen de différents outils à la fois efficaces et légaux.

Bien évidemment, les « vrais méchants » que sont les terroristes, djihadistes, gangsters et autres trafiquants connaissent et utilisent déjà ces outils : vous vous doutez bien qu'ils n'ont pas attendu ce billet de blog pour les découvrir...

[x]

Une boîte à outils pour protéger votre vie privée

Anonymat sur Internet

Pour protéger votre identité sur Internet et notamment sur le web, vous pouvez combiner l'utilisation d'un réseau privé virtuel, ou VPN, et de TOR, un système d'anonymisation qui nécessite l'installation d'un logiciel spécifique, TOR Browser. Je ne vous donne pas de référence particulière en matière de VPN, car l'offre est pléthorique.

MAJ : un lecteur m'a indiqué l'existence de La brique Internet, un simple boîtier VPN couplé à un serveur. Pour que la Brique fonctionne, il faut lui configurer un accès VPN, qui lui permettra de créer un tunnel jusqu'à un autre ordinateur sur Internet. Une extension fournira bientôt aussi en plus un accès clé-en-main via TOR en utilisant la clé wifi du boîtier pour diffuser deux réseaux wifi : l'un pour un accès transparent via VPN et l'autre pour un accès transparent via Tor.

Chiffrement des données

Pour chiffrer le contenu de vos données, stockées sur les disques durs de vos ordinateurs ou dans les mémoires permanentes de vos smartphones, vous pouvez mettre en œuvre des outils tels que LUKS pour les systèmes Linux ou TrueCrypt pour les OS les plus répandus : même si TrueCrypt a connu une histoire compliquée, son efficacité ne semble pas remise en cause par le dernier audit de code effectué par des experts.

Je vous signale aussi que l'ANSSI – Agence nationale de la sécurité des systèmes d'information – signale d'autres outils alternatifs comme Cryhod, Zed !, ZoneCentral, Security Box et StormShield. Même si l'ANSSI est un service gouvernemental il n'y a pas de raison de ne pas leur faire confiance sur ce point ☐

Chiffrement des e-mails et authentification des correspondants

GPG, acronyme de GNU Privacy Guard, est l'implémentation GNU du standard OpenPGP. Cet outil permet de transmettre des messages signés et/ou chiffrés ce qui vous garantit à la fois l'authenticité et la confidentialité de vos échanges. Des modules complémentaires en facilitent l'utilisation sous Linux, Windows, MacOS X et Android.

MAJ : un lecteur m'a signalé PEPS, une solution de sécurisation française et Open Source, issue d'un projet mené par la DGA – Direction générale de l'armement – à partir duquel a été créée la société MLState.

Messagerie instantanée sécurisée

OTR, Off The Record, est un plugin à greffer à un client de messagerie instantanée. Le logiciel de messagerie instantanée Jitsi, qui repose sur le protocole SIP de la voix sur IP, intègre l'outil de chiffrement ZRTP.

Protection des communications mobiles

A défaut de protéger les métadonnées de vos communications mobiles, qu'il s'agisse de voix ou de SMS, vous pouvez au moins chiffrer les données en elles-mêmes, à savoir le contenu de vos échanges :

RedPhon est une application de chiffrement des communications vocales sous Android capable de communiquer avec Signal qui est une application du même fournisseur destinée aux iPhone sous iOS.

TextSecure est une application dédiée pour l'échange sécurisé de SMS, disponible pour Android et compatible avec la dernière version de l'application Signal. Plus d'information à ce sujet sur le blog de Stéphane Bortzmeyer.

MAJ : un lecteur m'a indiqué l'application APG pour Android qui permet d'utiliser ses clés GPG pour chiffrer ses SMS.

Allez vous former dans les « cafés Vie Privée »

Si vous n'êtes pas geek et ne vous sentez pas capable de maîtriser ces outils sans un minimum d'accompagnement, alors le concept des « cafés Vie Privée » est pour vous : il s'agit tout simplement de se réunir pour apprendre, de la bouche ceux qui savent le faire, comment mettre en œuvre les outils dont je vous ai parlé plus haut afin de protéger sa vie privée de toute intrusion, gouvernementale ou non.

Tout simplement, il s'agit de passer un après-midi à échanger et à pratiquer la cryptographie. Pour cela sont proposés des ateliers d'une durée minimum de 1 heure, axés autour de la sécurité informatique et de la protection de la vie privée.

Et comme le disent avec humour les organisateurs, « les ateliers sont accessibles à tout type de public, geek et non-gEEK, chatons, poneys, loutres ou licornes. ». Bref, le « café Vie Privée » est à la protection de la vie privée ce que la réunion Tupperware était à la cuisine ☐

[x]

Voilà, vous avez je l'espère suffisamment d'éléments pratiques pour commencer à protéger votre vie privée... en espérant vraiment que le Conseil Constitutionnel abrogera les points les plus contestables de cette loi et nous évitera d'avoir à déployer un tel arsenal sécuritaire.

PS : l'image « 1984 was not a manual » a été créée par Arnaud Velten aka @Bizcom.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : <http://www.zdnet.fr/actualites/loi-renseignement-la-bo-te-a-outils-pour-apprendre-a-protecter-votre-vie-privee-en-chiffrant-vos-donnees-et-communications-39818894.htm>
Par Pierre Col

Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 | Denis JACOPINI

 **Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 2h24**

Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la #cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en #sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

La Commission Européenne facilite l'accès aux preuves électroniques

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

LE NET EXPERT
AUDITS & EXPERTISES

EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES
LENETEXPERT.fr

RGPD CYBER

SPY DETECTION
Services de détection
de logiciels espions

LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

Denis JACOPINI

vous informe

La Commission Européenne, facilite l'accès aux preuves électroniques

La Commission propose de nouvelles règles visant à permettre aux autorités policières et judiciaires d'obtenir plus facilement et plus rapidement les preuves électroniques, comme les courriels ou les documents se trouvant sur le cloud, dont elles ont besoin pour mener à bien leurs enquêtes, ainsi que pour poursuivre et condamner les criminels et les terroristes.

Les nouvelles règles permettront aux services répressifs des États membres de l'UE de mieux rechercher des pistes en ligne et par-delà les frontières, tout en offrant des garanties suffisantes pour les droits et les libertés de tous les intéressés.

M. **Frans Timmermans**, premier vice-président de la Commission, a déclaré à ce propos: «*Les preuves électroniques revêtent une importance croissante en matière pénale. Nous ne pouvons pas accepter que les criminels et les terroristes exploitent les technologies de communication électroniques modernes pour dissimuler leurs actes et se soustraire à la justice. Les criminels et les terroristes ne doivent pouvoir trouver aucun refuge en Europe, que ce soit en ligne ou hors ligne. Les propositions présentées aujourd'hui visent non seulement à mettre en place de nouveaux instruments qui permettront aux autorités compétentes de recueillir des preuves électroniques rapidement et efficacement par-delà les frontières, mais aussi à assurer des garanties solides pour les droits et les libertés de toutes les personnes concernées.*»

Les propositions visent à:

- créer une injonction européenne de production ;
- empêcher l'effacement de données au moyen d'une injonction européenne de conservation ;
- mettre en place des garanties solides et des voies de recours ;
- contraindre les prestataires de services à désigner un représentant légal dans l'Union ;
- procurer une sécurité juridique aux entreprises et aux prestataires de services ;

[L'article original complet]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Commission Européenne – COMMUNIQUES DE PRESSE – Communiqué de presse – Union de la sécurité: la Commission facilite l'accès aux preuves électroniques*



Non, NotPetya n'est pas un ransomware... mais un logiciel de sabotage



Le déchiffrement des machines impactées est impossible. La demande de rançon n'était donc qu'un leurre pour camoufler un cybersabotage. La piste d'un acte politique, probablement réalisé par une agence gouvernementale, émerge.

Mauvaise nouvelle pour toutes les victimes de NotPetya. Les dernières analyses des chercheurs en sécurité montrent que ce malware est en réalité un logiciel de sabotage déguisé en ransomware. Les victimes ne pourront donc retrouver leurs données, à moins qu'un expert arrive à détecter une faille dans le processus de chiffrement.

Plusieurs indices prouvent que les auteurs de NotPetya n'ont jamais eu l'intention d'envoyer une quelconque clé de déchiffrement. Le premier concerne l'identifiant unique affiché dans le message de rançonnage et que la victime doit envoyer aux pirates après avoir effectué le paiement en bitcoins. En théorie, cet identifiant doit permettre aux auteurs de NotPetya d'identifier la victime. Il doit, par conséquent, contenir des informations sur les clés de chiffrement utilisées sur la machine en question. Mais selon les chercheurs de Kaspersky, il s'avère que cet identifiant est totalement aléatoire. « *Les attaquants ne peuvent extraire une quelconque information de déchiffrement d'une telle suite de caractères aléatoire* », soulignent-t-ils dans une note de blog.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Mz7153HMuXTuR2R1t78mGSdzaRtNbBLX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith12345@posteo.net. Your personal installation key:
BSENwb-CPccj7-SwaiAC-9UPieg-KA3Hyw-ND9fd8-suq54i-TAxTS8-M2oaT6-6ADSBF

If you already purchased your key, please enter it below.
Key:

Kaspersky – L'identifiant unique affiché est totalement aléatoire

De son côté, le chercheur en sécurité Matt Suiche a découvert que les données de la zone d'amorçage ne sont sauvegardées nulle part, mais simplement remplacées par autre chose. Le système de fichier du disque serait donc de toute façon irrécupérable. « *La version actuelle de Petya a été réécrite pour être un wiper, et non un ransomware* », souligne l'expert...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Non, NotPetya n'est pas un ransomware... mais un logiciel de sabotage*

Voilà la prochaine cyberattaque



Voilà la prochaine cyberattaque

Après WannaCry et ses 200.000 demandes de rançon, une nouvelle cyberarme cible les réseaux électriques. Où sont les failles? Nos industries sont-elles parées? Enquête exclusive.

À lui seul, son nom file déjà des frissons. Baptisé "Industroyer" (contraction des termes anglais "industrial" et "destroyer"), un nouveau virus vient d'être identifié par des chercheurs en sécurité informatique. Il s'agit d'un puissant logiciel malveillant, voire une cyberarme de destruction massive. Ce virus industriel cible en effet le secteur de l'énergie. "C'est même la menace la plus puissante pour les systèmes de contrôle industriels depuis Stuxnet!", enchérit le spécialiste slovaque en cybersécurité ESET, codécouvreur de cette nouvelle menace avec l'américain Dragos.

Pour rappel, le ver informatique Stuxnet, attribué aux services secrets américains et israéliens, a saboté une centrale nucléaire iranienne en 2010, provoquant même des explosions. Une première mondiale dans l'histoire du piratage informatique, qui aurait pu se solder selon les experts russes par un accident pire que celui de Tchernobyl. Le potentiel de cette super-mine numérique? D'après ces chercheurs européens et américains, Industroyer serait déjà responsable du piratage du réseau ukrainien en décembre 2016, qui avait privé une partie de Kiev d'électricité pendant plus d'une heure. "Ce nouveau virus peut être immédiatement adapté pour attaquer des réseaux en Europe et dans une partie du Moyen-Orient et de l'Asie", avertit encore l'expert US. Cette cyberarme peut-elle dès lors frapper la Belgique, pays fortement nucléarisé et très densément électrifié? Se couvrant derrière le secret-défense, aucun opérateur belge ne se risque à y répondre...[lire la suite]

Bref commentaire de Denis JACOPINI :

Les années nous ont donné raison, nous les lanceurs d'alertes qui sensibilisons les décideurs et les élus depuis des années en tirant la sonnette d'alarme pour anticiper les risques. Chaque jour qui passe nous donne raison nous comptons les victimes de la cybercriminalité par milliers.

Le cybercrime peut prendre de nombreuses apparences, mais les décideurs et les élus, pénallement responsables aussi bien des fuites de données que de la perte des données doivent prendre les devants. Fort de nos années d'expérience dans ce domaine, nous organisons, en collaboration avec les CCI, les clubs d'entreprises et les centres de formations des sessions de sensibilisation aux risques informatiques et à la mise en conformité de vos données personnelles.

Contactez-nous

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- [Audits RGPD](#)
- [Accompagnement à la mise en conformité RGPD](#)
- [Formation de Délégués à la Protection des Données](#)
- [Analyse de risques \(ISO 27005\)](#)
- [Expertises techniques et judiciaires ;](#)
- [Recherche de preuves](#) téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- [Expertises de systèmes de vote électronique](#) ;

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en
Protection des Données Personnelles

[Contactez-nous](#)

ou suivez nous sur



Réagissez à cet article

Les entreprises du CAC 40 sont la cible de cyberattaques



Les entreprises du CAC 40 sont la cible de cyberattaques

Renault n'est pas la seule entreprise dans le viseur des cyberterroristes. Les champions de la défense et les géants de la Bourse peaufinent leur bouclier.

par GuerriC PONCET

« En 2016, de gros industriels ont été touchés et des géants du CAC 40 ont pris conscience qu'ils pouvaient disparaître du jour au lendemain à cause d'une cyberattaque », nous confie Guillaume Poupart, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). « Je veux dire que, si leur piratage était dévoilé, ils étaient *OPAble*s le lendemain », précise-t-il. En effet, la révélation d'une telle attaque ferait immédiatement chuter le cours de la Bourse...

Nos champions de la cybersécurité, Airbus, Thales, Capgemini et Orange en tête, sont sollicités de toutes parts par les comités exécutifs. Mais leurs tarifs sont souvent hors de portée des PME : dans le cyber, la défense coûte cent fois le prix de l'attaque. Et, quand bien même, le budget ne fait pas tout : JP Morgan, Yahoo !, Adobe, Visa ou encore Sony ont beau avoir alloué des centaines de millions de dollars à leur sécurité informatique, ils ont tous vécu des intrusions gravissimes. « Il est impossible de créer un cyberbouclier infailible », tranche Guillaume Poupart, pour qui il faut avoir « une bonne gouvernance avant même de parler technique ». « Jusqu'à présent, nous avons stoppé les attaques majeures qui nous visaient, mais, si l'une d'elles réussissait, ce serait une catastrophe, avec des conséquences sur la souveraineté économique de la France et, très rapidement, sur la sécurité des populations », nous glisse, sous le couvert de l'anonymat, le responsable de la sécurité informatique d'une entreprise classée « opérateur d'importance vitale » (OIV).

Des exercices de crise sont régulièrement menés pour anticiper et limiter les dégâts que créerait assurément une cyberattaque chez un OIV – panne générale dans la production électrique, paralysie des transports, implosion des télécoms... Des agents de l'Anssi jouent aux hackers, tentent de déjouer les systèmes de sécurité... et y parviennent : « La dernière fois, ils ont pris le contrôle d'une partie de notre système assez facilement, ils auraient pu créer des accidents graves », reconnaît, lui aussi en toute discrétion, le responsable informatique d'un autre OIV. Nous voilà rassurés...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« **Cybercriminalité** » et en **RGPD** (Protection des Données à Caractère Personnel).



- **Audits RGPD**
- **Accompagnement à la mise en conformité RGPD**
- **Formation de Délégués à la Protection des Données**
- **Analyses de risques (ISO 27005)**
- **Expertises techniques et judiciaires ;**
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en
Protection des Données Personnelles

[Contactez-nous](#)

ou suivez nous sur



Réagissez à cet article

Source : *Cyberguerre : le CAC 40 dans le viseur* – Le Point

La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation



La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

Face à la vague d'attentats qui frappe l'Europe, la Commission européenne discute actuellement de quelques changements dans les réglementations afin de permettre aux forces de Police d'accéder aux données des utilisateurs des services de Google et Facebook, sans autorisation préalable d'un Juge.

Les vagues d'attentat et la peur ambiante sont bien souvent l'occasion pour les gouvernements de voter des lois liberticides, et ce pourrait à nouveau être le cas dans toute l'Europe. La Commission européenne réfléchit actuellement à changer les réglementations afin de permettre aux forces de police d'aller piocher des informations dans les comptes des réseaux sociaux des utilisateurs, sans accord préalable de qui que ce soit.



Concrètement, le projet évoque même la possibilité pour les policiers d'origine étrangère de consulter les données privées des profils de ces réseaux sociaux, afin notamment d'enquêter sur un touriste ou une personne d'un autre pays de l'Union européenne. Exemple : vous partez en Italie pour quelques jours et vous faites arrêter par la police locale, ces derniers pourraient alors éplucher vos profils sociaux pour tenter d'obtenir plus d'informations sur vous, et ce, sans rien demander à la France.

Actuellement, trois projets de ce type ont été proposés et soumis à étude, l'un d'entre eux pouvant être adopté d'ici la fin de l'année 2018. Une des propositions évoque la possibilité de copier les données directement depuis le Cloud de la plateforme sociale afin d'en faire une sauvegarde et éviter la disparition des données en cas d'enquête...[lire la suite]



Commentaire de Denis JACOPINI

Entre Facebook qui analyse et espionne ses membres et les OPJ (Officiers de Police Judiciaire) qui peuvent consulter les données collectées par Facebook, il n'y a qu'un pas pour que ce même type de démarche soit aussi engagée auprès de Google pour qu'on nous mette des radars automatiques sur Internet qui nous flashent dès que quelqu'un en train picoler publie une photo.

Sans plaisanter, ces projets de loi consistent à permettre à des OPJ d'accéder aux zones privées de Facebook, car vous savez que lorsque vous publiez quelque chose sur Facebook, cet ajout peut être public (tout le monde peut le consulter et le voir) ou privé et il n'y a qu'un juge qui peut forcer Facebook à communiquer le contenu privé d'un compte. Ce projet ne changera rien pour ceux qui n'ont rien à se reprocher, et pas grand chose pour ceux qui ont quelques choses à se reprocher. Les OPJ pourront disposer plus rapidement des contenus privés pour alimenter leurs enquêtes.

Il est fort probable à l'avenir qu'un autre réseau social soit utilisé par les malfrats l'histoire de faire courir le chat...

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- [Audits RGPD](#)
- [Accompagnement à la mise en conformité RGPD](#)
- [Formation de Délégué à la Protection des Données](#)
- [Analyse de risques \(ISO 27005\)](#)
- [Expertises techniques et judiciaires](#) ;
- [Recherche de preuves](#) téléphones, disques durs, emails, conteneurs, détournements de clientèle... ;
- [Expertises de systèmes de vote électronique](#) ;



[Contactez-nous](#)



ou suivez nous sur

Réagissez à cet article

Source : *Europe : la Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation*

Limiter les risques venant des drones en les immatriculant. Une bonne idée ?



Limiter les risques venant des drones en les immatriculant. Une bonne idée ?

Horsile à une surveillance en réseau, le fabricant DJI propose une immatriculation électronique que seules les forces de l'ordre pourraient exploiter.

Jean-Michel Normand



L'idée trotte dans la tête de nombreux députés. Installer à bord des drones de loisir un système de reconnaissance électronique fait déjà partie de l'arsenal législatif adopté l'an passé par les parlementaires français, sans pour autant que des précisions techniques aient été définies. L'Italie et le Danemark ou la FAA, l'Aviation civile américaine, l'ont également inscrit à leur programme. Dans une proposition qu'il vient de rendre publique, le fabricant de drones chinois DJI préconise une identification électronique « simple, qui maintient un équilibre entre le respect de la vie privée de l'opérateur du drone et les légitimes préoccupations des autorités relatives à l'utilisation de ces appareils ».



1. Plusieurs pays, dont la France, envisagent d'imposer une signature électronique. NIR ELIAS / REUTERS

- Comparable à une plaque d'immatriculation automobile -

DJI est favorable à ce que tous les drones commerciaux soient capables d'émettre un signal qui indique leur localisation, mais aussi un code d'identification « comparable à une plaque d'immatriculation automobile » en mode électronique. Ce code serait émis sur les bandes de fréquence (2,4 GHz et 5,8 GHz) utilisées pour la liaison entre le drone et la radiocommande du pilote et pour la liaison vidéo. Il suffirait de réaliser une mise à jour des protocoles de contrôles radio existants. L'information pourrait être captée par la police ou un particulier furieux de voir un quadrirotor évoluer au-dessus de sa propriété, à condition qu'il soit équipé d'un récepteur adapté. Il lui faudra alors se tourner vers les forces de l'ordre, seules autorisées (avec les autorités aéroportuaires, notamment) à remonter jusqu'au titulaire de l'immatriculation électronique. [lire la suite]

Commentaire de Jean-Michel Normand :

1. Je trouve personnellement l'idée intéressante, encore faut-il que :
2. L'émission de cette information ne puisse pas être perturbée (j'en doute) ;
3. Cette procédure soit largifiée et suivie par tous les constructeurs mondiaux.

Ceci n'empêchera pas les groupes les plus obscurs d'utiliser des drones volés non pourvus de cette signature.

A mon avis, la mise en place de ces précautions ne concernent que l'utilisateur lambda, pas ceux que l'on craint actuellement le plus sur le territoire.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Commissariat Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 94 83941 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations/cyber/analyse-protection-des-donnees-personnelles>



Le Net Expert
INFORMATIQUE
Cybersecurité & Conformité

Réagissez à cet article

Source : *Comment immatriculer les drones de loisirs*

Risque de cyberattaque terroriste très élevé

Risque de
cyberattaque
terroriste
très élevé



© Dieter Telemans

Le commissaire chargé de la Sécurité nous explique ce que l'Europe a fait pour améliorer la sécurité de ses citoyens. Il avoue craindre « tous les types de menaces ».

Il est « Le Dernier des Mohicans ». L'ultime commissaire britannique envoyé par Londres avant le Brexit. Dans son bureau du Berlaymont placé sous haute sécurité, trônent deux grandes photographies de Sa Majesté. Sur le sofa, des coussins décorés de l'Union Jack. « No doubt », c'est bien ici une partie de l'île encore arrivée à l'Europe. Julian King, formé à la fois à Oxford et à l'ENA, est l'un des plus brillants diplomates du Royaume. Sa mission? Créer l'Union européenne de la sécurité ainsi que gérer la lutte contre le terrorisme et le crime. L'Echo l'a rencontré, un an après les attentats terroristes à Bruxelles.

Comment avez-vous vécu les attaques du 22 mars?

J'étais ambassadeur du Royaume-Uni en France. Je revenais du marché de Rungis. C'était tôt le matin. J'ai mis du temps à me remettre de cette nouvelle. Dès mon retour à la résidence, j'ai demandé qu'ils mettent le drapeau en berne.

Qu'avez-vous ressenti?

Je craignais de nouveaux attentats depuis mon entrée en fonction à Paris. C'est arrivé dans la capitale du pays voisin, là où ma femme vit et travaille. Son bureau n'était pas loin de Maelbeek. J'ai eu peur que mes amis m'appellent pour m'apprendre une mauvaise nouvelle.

Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Qu'est-ce que les attentats ont changé?

Après chaque attaque, à Paris, Bruxelles et Nice, j'ai été frappé de voir à quel point nos villes sont résilientes. Ces événements sont horribles. Très difficiles à vivre pour les victimes mais aussi pour les gens qui doivent monter en première ligne et tous les habitants de la ville. Je suis touché par la capacité des Belges et des Français à dépasser le drame. À reprendre leur vie. Et le lien profond qu'ils ont avec leur communauté.

Qu'a fait l'Europe, depuis lors, pour améliorer la sécurité de ses citoyens?

Nous avons commencé par renforcer les frontières extérieures. Nous avons créé un corps de garde-frontières et de garde-côtes, déployé du personnel de Frontex et d'Europol pour soutenir les autorités en Grèce et en Italie, adopté une directive sur le contre-terrorisme qui criminalise les allers-retours d'Irak et de Syrie. Nous avons renforcé le code Schengen pour contrôler systématiquement toute personne qui entre dans l'espace Schengen, y compris les citoyens Européens.

Nous avons proposé de créer un système interactif pour contrôler les nationaux des pays tiers, c'est à l'étude au Parlement. Nous allons aussi mettre en place un système de précontrôle des étrangers n'ayant pas besoin de visas, appellé Etias et calqué sur le modèle Etas des Etats-Unis.

Nous avons renforcé notre capacité de connaître ceux qui arrivent dans l'espace européen, et c'est un élément vital pour notre sécurité.

Qu'avez-vous fait pour accroître la sécurité intérieure?

Nous avons renforcé les capacités des forces de l'ordre. Nous avons mis plus d'argent, de personnel et de moyens dans Europol. Nous avons consolidé les bases de données policières et réformé la plus importante: le système Schengen. Nous voulons obliger les polices nationales à partager leurs informations à travers ce système. Dans les faits, ils le font de plus en plus. Mais ce sera encore plus vrai lorsque l'obligation d'échanger sera adoptée par le Conseil européen.

Nous devons aussi accroître la capacité des agents d'aller chercher une information là où elle se trouve.

Pour éviter, comme après les attaques de Paris, qu'un terroriste comme Salah Abdeslam puisse déjouer les contrôles...

Oui. Les renseignements existaient mais lors de ce fameux contrôle entre Paris et Bruxelles, la police n'a pas été capable d'aller les chercher. Nous allons proposer un paquet de mesures pour améliorer la qualité des informations, le traitement de données, l'utilisation plus fréquente de la biométrie et accroître la rapidité d'obtention des informations.

La moitié des business européens ont déjà subi une cyber-attaque.

Quand allez-vous proposer ces mesures?

Mon équipe y travaille, son rapport devrait être prêt d'ici avril. Nous ferons ensuite des propositions.

Les États européens appliqueront-ils ces mesures?

Nous insistons beaucoup là-dessus. Pour la première fois depuis mon arrivée l'été dernier, la Commission a lancé des procédures d'infraction contre plusieurs États qui n'appliquent pas les mesures convenues l'an dernier. Trois procédures contre des États qui n'ont pas appliqué la directive sur les explosifs et cinq procédures contre des États qui n'ont pas appliqué l'arrangement de Prüm sur les échanges d'information.

Que pensez-vous de la création d'un « FBI Européen », comme le préconise Guy Verhofstadt?

Je ne suis pas persuadé que cela arrive dans un futur immédiat. Il y a des questions légales, des difficultés constitutionnelles à lever. Mon objectif, pour le moment, est de construire une coopération pratique entre les agences de renseignements nationales. Certains prétendent qu'il n'existe aucun échange entre elles, mais ce n'est pas vrai. Cette collaboration existe, les agences européennes ont d'ailleurs depuis peu une plateforme commune aux Pays-Bas.

Vous n'aimez pas parler du Brexit. Mais dites-moi, le Royaume-Uni continuera-t-il à coopérer avec l'UE après son départ?

Je l'espère. Je ferai tout durant les deux années à venir pour renforcer notre sécurité commune contre le terrorisme, le cyberterrorisme et le crime organisé. Ces menaces affectent tous les pays d'Europe, qu'ils soient ou pas dans Schengen ou dans l'UE, et c'est le cas en particulier des cyberattaques. Notre combat sera plus efficace si nous le menons ensemble. Ce sera vrai demain, dans deux ans et dans cinq ans. Il est important qu'après le Brexit l'Union européenne et le Royaume-Uni conservent une coopération étroite en matière de lutte contre le terrorisme.

Quant à la coopération entre l'Europe et les Etats-Unis, résistera-t-elle à l'arrivée de Donald Trump?

Jusqu'à présent, tous les représentants des Etats-Unis que j'ai rencontrés ont été clairs. Ils comprennent l'importance de notre coopération et veulent la maintenir.

Quel est le niveau de risque d'attentat terroriste à Bruxelles?

Nous ne sommes pas chargés d'évaluer ce niveau, mais nous écoutons ce que chaque État nous dit. Et il est clair que la menace terroriste dans un État qui a subi une attaque est très très élevée. Il est très important de ne pas donner l'impression que la menace a disparu. Ou que nous avons réduit la menace à zéro.

Les terroristes se concentrent sur les espaces publics, les métros ou les aéroports. Comment sécuriser de tels lieux?

Chaque État a développé de très bonnes pratiques dans la gestion de la sécurité des espaces publics. Nous mettons ensemble tous les experts pour tirer les leçons des meilleures pratiques et nous dressons une liste de lignes directrices. Nous allons continuer ce travail et le faire avec les meilleurs praticiens.

Vous craignez des menaces d'isolés ou des groupes organisés?

Tous les types de menaces. Celles de loups solitaires, et c'est pourquoi la lutte contre la radicalisation est une partie importante de nos travaux. Mais aussi les menaces d'attaques inspirées par Daech, qui ne sont pas réduites parce qu'ils sont en difficulté sur le terrain en Syrie et en Irak.

La plupart des auteurs des attaques à Bruxelles et Paris étaient Européens.

Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Que fait l'Europe pour lutter contre la radicalisation?

Nous agissons à deux niveaux. D'abord nous nous attaquons à la propagande de Daech sur internet, qu'ils continuent à déverser malgré leur déroute sur le terrain. Nous travaillons pour l'instant avec les plus grands groupes du web. Nous avons besoin de leur aide pour trouver des moyens industriels qui arrêtent cette propagande.

L'autre risque majeur ce sont les gens qui, au sein des communautés, cherchent à pousser les plus fragiles à la violence. Le moyen le plus efficace pour les empêcher d'agir est de travailler localement. Nous avons développé, au niveau européen, des moyens pour œuvrer avec ces communautés, soit par des fonds, soit par la mise en place d'un réseau d'organisations où ils reçoivent du soutien.

Craignez-vous une cyberattaque terroriste, par exemple contre une centrale nucléaire ou une tour de contrôle aérienne?

Tes terroristes comme Daech n'utilisent pas, pour l'instant, de tels moyens. Mais le risque d'une cyberattaque terroriste est très élevé. La cybersécurité augmente de manière exponentielle. Au Royaume-Uni, un pays que je connais bien, la moitié des crimes connus sont des cybercrimes. Si vous regardez l'Europe, la moitié des business européens ont déjà subi une cyberattaque.

Comment affrontez-vous ce risque?

Notre première ligne de défense consiste à avertir le public du danger de manipulation sur internet. Nous devons ensuite construire une résilience, à chaque niveau. Apprendre aux individus à protéger leurs appareils, changer leur code. Il faut aussi mettre en place les moyens nécessaires pour protéger les infrastructures critiques, comme les unités de production d'énergie, exposées aux cyberattaques. Nous travaillons à la création d'une agence européenne qui planifie la protection des infrastructures et mette en place un réseau d'échange d'information, le tout en application de la directive NIS.

Nous travaillons aussi avec le secteur privé, généralement très avancé sur ces questions de sécurité, et lancer des partenariats. Nous allons mobiliser 1,8 milliards d'euros pour des recherches en cybersécurité d'ici 2020. C'est un effort important.

Nous préparons également des exercices conjoints avec l'Otan pour contrer les cyberattaques.

Enfin, j'espère que nous pourrons faire un examen complet de tout notre travail sur la cybersécurité sous présidence estonienne, avant la fin de cette année...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement... [Autorisations de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03641 84]

Plus d'informations sur : <https://www.netexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Denis JACOPPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en Protection des Données et Confidentialité Personnelle. • Audit et conseil ISO 27001 ; • Expertises techniques et judiciaires (Avus techniques, Recherche de preuves téléphones, dispositifs mobiles, ordinateurs, conteneurs, débrouillages de clientèle...) ; • Expertises de systèmes de vote électronique ; • Formations et conférences en cybercriminalité ; • Formation à la RGPD et au CIL ; • Formation de CIL (Correspondants Informatique et Libertés) ; • Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : « *Le risque d'une cyberattaque terroriste est très élevé* » | *L'Echo*