Risque de cyberattaque terroriste très élevé

 © Dieter Telemans	**Risque de cyberattaque terroriste très élevé**

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 arrimée 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, appelé Etias et calqué sur le modèle Esta 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 organisées inspirées par Daech, qui ne sont pas réduites parce ce 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 pas 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?
Les terroristes comme Daech n'utilisent pas, pour l'instant, de tels moyens. Mais le risque d'une cyberattaque terroriste est très élevé. La cybercriminalité 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 cyberattaque.
*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.. (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 DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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

Le ministère de la Défense confirme l’augmentation des tentatives de piratage informatique

Le ministère de la Défense confirme l’augmentation des tentatives de piratage informatique

---

L'armée sud-coréenne a récemment été la cible de tentatives accrues de piratage informatique sur fond de relations tendues avec la Chine et de comportement belliqueux de la Corée du Nord, a fait savoir ce mardi le porte-parole du ministère de la Défense Moon Sang-gyun.
«Récemment, les tentatives d'intrusion dans (notre) système informatique se sont quelque peu accrues», a déclaré le porte-parole lors d'un point de presse, tout en notant qu'il n'y a eu aucun dégât subi. Il n'a toutefois pas précisé l'origine des cybermenaces évoquées.
Plus tôt dans la journée, un quotidien sud-coréen a rapporté que le nombre de cyberattaques contre l'armée sud-coréenne a fortement augmenté depuis que celle-ci a acquis le mois dernier un terrain de golf du groupe Lotte, dans le sud-est du pays, pour le déploiement du système de défense antimissile à haute altitude THAAD (Terminal High Altitude Area Defense) des Etats-Unis. La Chine est fortement opposée au plan des deux pays alliés de renforcer leur capacité à intercepter les missiles nord-coréens.
Le nombre de tentatives de piratage informatique contre le réseau informatique de l'armée a été de 44 entre les 9 et 15 mars, selon le rapport. Moon n'a pas confirmé ce chiffre.
Il a écarté les inquiétudes sur l'éventuelle vulnérabilité de l'intranet de l'armée, en soulignant qu'il est complètement «séparé» du serveur Internet.
L'intranet de l'armée a subi pour la première fois une cyberattaque en septembre dernier dont le Nord serait également à l'origine.
lsr@yna.co.kr

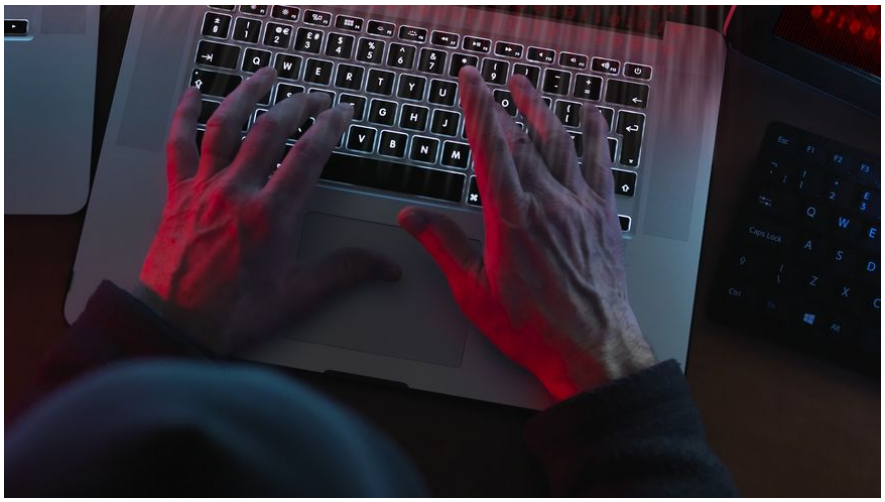
Réagissez à cet article

Source : *Le ministère de la Défense confirme l'augmentation*

des tentatives de piratage informatique | Agence de presse Yonhap

---

Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle



Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

---

Elles ont beaucoup fait parler d'elles durant la campagne présidentielle américaine : certaines pratiques malveillantes sur Internet pourraient aussi peser sur l'élection en France. Voici en quoi elles consistent.
Interview par Marina Cabiten (France Bleu)

Des pirates informatiques qui œuvrent contre Hillary Clinton, et donc en faveur de Donald Trump, le tout commandité par le Kremlin : il ne s'agit pas d'un scénario de film mais d'une accusation très sérieuse formulée par les autorités américaines lors de la campagne présidentielle. Internet est un outil puissant pour les manipulations informatiques, à différents degrés. Et la France est, selon plusieurs acteurs de la cybercriminalité, très mal préparée à ces usages détournés. Voici comment des personnes mal intentionnées pourraient perturber la campagne.

Inonder les réseaux sociaux de faux utilisateurs : l'astroturfing

Tout un chacun peut utiliser son compte Facebook ou Twitter pour s'exprimer, et éventuellement partager ses opinions politiques. Mais cette utilisation des réseaux sociaux peut être bidonnée. Ce phénomène est appelé astroturfing, du nom d'une marque de pelouse synthétique pour les stades : Astroturf. Autrement dit, il s'agit de faire prendre aux internautes du faux gazon pour de l'herbe naturelle… Comment ? **En inondant les réseaux sociaux de faux comptes automatisés, les "bots"**, qui diffusent des messages rédigés par les initiateurs de cette technique de "marketing politique" qui ne dit pas son nom, et garantit l'anonymat.
N'importe quel internaute peut créer et animer des faux comptes. Avec un peu plus de moyens financiers, il peut payer pour qu'un réseau social comme Facebook donne plus de visibilité à une page ou à un post via un algorithme qui fera apparaître le message sur davantage de "murs" d'utilisateurs, qui n'ont rien demandé. Sur Twitter, il peut acheter des "followers" (personnes qui suivent le compte) pour donner une fausse légitimité à ses comptes artificiels. Le degré ultime est de se payer un logiciel qui fait ça tout seul, voire d'employer quelqu'un pour l'exploiter. Cela existe, au sein d'entreprises privées mais parfois aussi de partis politiques. **C'est une forme de propagande de plus en plus répandue.** Le gouvernement français a annoncé récemment son intention de surveiller les réseaux sociaux pour éventuellement repérer des "mouvements" suspects de ce type.

Quand des sites partisans se font passer pour des organes de presse : les « fake news »

L'expression "Fake news", qui se traduit littéralement par « fausses informations », est très en vogue depuis la présidentielle américaine et vient de la diffusion sur Internet de prétendus articles de presse, qui ne sont en réalité pas rédigés par des journalistes. Des articles contenant des informations non vérifiées, parfois erronées, voire carrément mensongères dans le but bien précis de manipuler l'opinion.
La mécanique est la même que pour l'astroturfing, tout faire pour que ces "fake news" soient largement vues sur Facebook et les autres réseaux sociaux ou forums. Selon les calculs du site Buzzfeed, les articles relayant de fausses informations **(comme le faux soutien du pape François à Donald Trump, ou la révélation imaginaire de ventes d'armes par Hillary Clinton à l'organisation Etat islamique)** ont suscité 8,7 millions d'interactions sur Facebook durant la campagne américaine, contre 7,3 millions pour les articles de la presse traditionnelle.
En France récemment, plusieurs médias ont fait part de leur volonté de lutter contre ce phénomène, allant même pour certains jusqu'à nouer un partenariat avec Facebook et Google. ***"Le problème c'est que la rumeur court toujours beaucoup plus vite que la rectification ou la suppression du contenu"***, objecte Denis Jacopini, diplômé en cybercriminalité et sécurité de l'information, ***"laissant s'installer dans l'esprit de l'électeur ces fausses affirmations."***

De vrais contenus, mais dérobés et diffusés sans autorisation : le vol de données

La menace la plus sophistiquée reste le vol d'informations numériques. C'est l'exemple des pirates informatiques (hackers) qui ont récupéré près de 20.000 courriels de responsables du parti d'Hillary Clinton. Ils sont entrés dans les serveurs du parti démocrate dès l'été 2015, accumulant ces données parfois embarrassantes sans que personne ne s'en aperçoive, pour les publier au moment opportun pour déstabiliser le camp démocrate. Une cyberattaque venue de Russie pour aider Donald Trump à gagner l'élection, affirme la CIA dans un rapport révélé par la presse américaine. ***"Aucun parti politique français n'est actuellement protégé contre une telle malveillance"***, assure Denis Jacopini.
Selon le Canard Enchaîné (numéro du 8 février 2017), **les services secrets français s'inquiètent de cyberattaques russes** durant la Présidentielle, qui auraient pour but d'aider la campagne de Marine Le Pen. De son côté, le secrétaire général du mouvement « En Marche ! » Richard Ferrand a affirmé publiquement que les pirates russes visent particulièrement Emmanuel Macron et ont déjà attaqué à plusieurs reprises son site web.

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle*

Cyberattaques des présidentielles. Qui serait responsable ?

Les cyber-attaques que la Russie est soupçonnée de mener en France dans le cadre de la campagne présidentielle sont « une forme d'ingérence inacceptable », a estimé dimanche le ministre français des Affaires étrangères Jean-Marc Ayrault.

» Les cyberattaques russes, grande menace pour les États-Unis et l'Europe
Dans une interview au *Journal du Dimanche*, le chef de la diplomatie française a déclaré : « Il suffit de regarder pour quels candidats, à savoir Marine Le Pen ou François Fillon, la Russie exprime des préférences, dans la campagne électorale française, alors qu'Emmanuel Macron, qui développe un discours très européen, subit des cyberattaques. Cette forme d'ingérence dans la vie démocratique française est inacceptable et je la dénonce ».
« La Russie est la première à rappeler que la non-ingérence dans les affaires intérieures est un principe cardinal de la vie internationale. Et je la comprends. Et bien la France n'acceptera pas, les Français n'accepteront pas qu'on leur dicte leurs choix », a ajouté le ministre.

Quels éléments a-t-on pour de telles affirmations ?
Denis JACOPINI : Aujourd'hui la Russie, hier la Chine et demain qui ? Quels sont les éléments permettant d'affirmer de tels propos ?
L'adresse IP ?
Si c'est l'adresse IP qui est prise en compte, n'est-on nous pas en train de mélanger l'adresse IP ayant accédé aux systèmes informatiques et celle du commanditaire de l'attaque ?
Signatures et codages de caractères
Si ce sont les signatures présentes dans les codes ou les codages de caractères qui sont pris en compte, ne risque t-on pas de reproduire l'attribution hâtive de l'attaque de la chaîne TV5 monde à l'Etat islamique
alors même que très vite après l'attaque, de nombreux experts avaient mis en doute la crédibilité de la revendication.
A mon avis
En raison du refus de certains pays pour coopérer en matière de lutte contre la cybercriminalité, il devient très compliqué de remonter jusqu'aux ordinateurs utilisés pour mener de telles attaques, pire encore pour remonter jusqu'aux commanditaires des attaques informatiques. Les infos circulant encore ce matin font référence une fois de plus à des accusations qui sembleraient bien être sans preuve…
Malgré l'absence de preuve, Ayrault dénonce une «ingérence» de la Russie dans la présidentielle
Je serais bien intéressé
En tant qu'Expert judiciaire spécialisé en cybercriminalité, je serais bien intéressé pour expertiser les éléments concernés par cette affaire.
A bon entendeur…

Qu'en pensez-vous ? Merci de me laisser votre avis ou commentaire

---

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Paris dénonce à nouveau les cyberattaques de Moscou*

Le fonctionnement d'Internet ne tient qu'à (presque) un fil

Le fonctionnement d'Internet ne tient qu'à (presque) un fil

Original de l’article mis en page : « Qui a le savoir, a le pouvoir »: Les câbles sous-marins, le maillon faible de la cyberguerre

---

Crainte de cyberattaques lors les élections présidentielles Françaises

R

Crainte de cyberattaques lors les élections présidentielles Françaises

---

Jean-Yves Le Drian a annoncé que 24.000 cybertattaques ont été déjouées en 2016, renforçant les craintes à quelques mois de la présidentielle.

La menace liée aux cyberattaques inquiète les pays occidentaux. Jean-Yves Le Drian a annoncé dans un entretien au *Journal du Dimanche* que 24.000 cybertattaques ont été déjouées en 2016, quelques jours après un rapport des services de renseignement américains pointant du doigt l'ingérence russe dans l'élection présidentielle américaine.

De quoi faire craindre des opérations similaires lors de la prochaine présidentielle en France, en avril et en mai prochain. « Il existe un risque à prendre très au sérieux que l'élection présidentielle soit menacée d'instrumentalisation par le biais d'attaques ou de propagande cyber », met en garde François Clémenceau, journaliste au *Journal du Dimanche* et auteur de l'interview.

« Les politiques ont pris des mauvaises habitudes. »

« Notre enquête auprès des formations politiques montre que la prise de conscience existe, mais elle est encore faible. Les personnalités politiques ont pris de très mauvaises habitudes dans l'utilisation de leurs téléphones et de leurs ordinateurs », s'inquiète-t-il.

Un risque d'attaque russe.

François Clémenceau affirme également que la France pourrait être victime d'une cyberattaque de la part de la Russie. « Ce qui est sûr, c'est que la France, comme l'Allemagne ou l'Italie, a une position vis-à-vis de la Russie sur l'Ukraine ou sur la Syrie… Il y a donc un intérêt du point de vue russe à déstabiliser une partie des démocraties occidentales, notamment en Europe et singulièrement la France, qui a pris des positions très dures par le biais de sanctions contre la Russie. »

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 de formation, de sensibilisation ou d'audits 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : « un risque d’instrumentalisation » de l’élection présidentielle

---

La Russie crée des unités d’élite de pirates informatiques

La Russie crée des unités d’élite de pirates informatiques

La Russie s'appuie sur les médiaux sociaux pour appeler de jeunes recrues à intégrer des « escadrons scientifiques » capables d'accéder à des systèmes et réseaux, à l'insu des cibles.
Accusée par les États-Unis d'avoir influencé l'élection américaine de novembre à travers des opérations de piratage informatique, la Russie a accéléré ses recrutements de pirates bien avant ces évènements, rapporte le *New York Times* en référence à une enquête du site d'information russophone Meduza. En plus de recruter dans les écoles d'ingénieurs, Moscou diffuse depuis plusieurs années des annonces sur les médias sociaux à l'attention d'étudiants et de programmeurs professionnels. Des hackers ayant maille à partir avec la justice sont également ciblés, selon Meduza.
L'une de ces annonces a été publiée sur le réseau social russe Vkontakte. Dans le spot vidéo ci-dessous, on devine un homme diposant d'une arme et d'un ordinateur portable. On peut y lire ce message : *« si tu es diplômé de l'enseignement supérieur, si tu es un spécialiste des technologies, nous t'offrons des opportunités, des équipements techniques de pointe, des capacités de calcul puissantes, du matériel dernier cri, un véritable entraînement au combat »*. Sans oublier le logement tout confort.

Former des « escadrons scientifiques »

Dans une autre annonce citée dans l'enquête, les autorités russes sont à la recherche d'informaticiens ayant des connaissances des *« patchs, vulnérabilités et exploits »*, explique Meduza, le site d'information russophone basé à Riga (Lettonie). La recherche de talents ne s'arrête pas là. Moscou se tournerait également vers des *« hackers ayant des problèmes avec la loi ».* Le gouvernement russe leur proposant une remise de peine en échange de leur engagement au service de la Russie…[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 de formation, de sensibilisation ou d'audits 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment la Russie crée des unités d’élite de pirates informatiques

---

Un logiciel malveillant russe découvert dans un ordinateur américain

Un logiciel malveillant russe découvert dans un ordinateur américain

Au lendemain de la passe d'armes diplomatique entre les Etats-Unis et la Russie, une entreprise américaine a fait savoir qu'un logiciel malveillant avait été découvert dans un de ses ordinateurs. Les autorités ont été alertées.
Nouvel élément dans la « guerre » que se mènent les Etats-Unis et la Russie ces derniers jours. Un programme malveillant associé à l'opération de piratage informatique russe, surnommée Grizzly Steppe par l'administration Obama, a été détecté dans un ordinateur portable lié à une compagnie d'électricité de l'Etat du Vermont. Celui-ci n'était cependant pas connecté au réseau électrique, a fait savoir l'entreprise Burlington Electric Department (BED).

« Nous avons pris aussitôt des mesures pour isoler l'ordinateur portable et avons alerté les autorités fédérales au sujet de la découverte », a dit l'entreprise BED, compagnie qui distribue l'électricité à Burlington dans le Vermont. « Notre équipe coopère avec les autorités fédérales pour remonter la piste de ce programme malveillant et empêcher toute autre tentative visant à s'introduire dans les ordinateurs du réseau électrique. Nous avons informé les autorités de l'Etat et coopérerons pleinement à l'enquête », a-t-elle ajouté.

Un seul cas connu

Le département américain de la Sécurité intérieure avait informé les compagnies d'électricité, jeudi 29 décembre, de l'existence du programme malveillant utilisé dans Grizzly Steppe. « Nous avons rapidement passé au crible l'ensemble des ordinateurs de notre système. Nous avons détecté le programme malveillant dans un seul ordinateur portable de Burlington Electric Department, non relié à la grille électrique de notre société », a indiqué la BED…[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 de formation, de sensibilisation ou d'audits 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : un logiciel malveillant russe découvert dans un ordinateur américain – LCI

Le réseau électrique américain pénétré par des pirates Russes

Le réseau électrique américain pénétré par des pirates Russes

Washington – Des pirates informatiques russes sont parvenus à pénétrer le réseau électrique américain via un fournisseur du Vermont, une cyberattaque sans conséquence sur les opérations de cette entreprise mais qui a pu révéler une « vulnérabilité », rapporte vendredi le Washington Post.

« Un code associé à l'opération de piratage informatique baptisée Grizzly Steppe par l'administration Obama a été détecté à l'intérieur du système d'un fournisseur d'électricité du Vermont », écrit le quotidien sur son site Internet, sans indiquer de date.
Se référant à des responsables américains non identifiés, il souligne que ce si code *« n'a pas été activement utilisé pour perturber les opérations du fournisseur* […] *la pénétration du réseau électrique national est importante parce qu'elle représente une vulnérabilité potentiellement grave ».*
Les autorités américaines ignorent à ce stade quelles étaient les intentions des Russes, poursuit le *Washington Post*, supputant qu'ils pourraient avoir tenté de porter atteinte aux activités du fournisseur –non identifié par les sources du journal– ou qu'il pourrait simplement s'agir d'un test de faisabilité.
Selon le journal, le Vermont compte deux importants fournisseurs d'électricité : Green Mountain Power et Burlington Electric.
Les pirates russes auraient envoyé des emails pour piéger les destinataires, leur faisant révéler leurs mots de passe.
En décembre 2015, 80 000 habitants de l'ouest de l'Ukraine avaient été plongés plusieurs heures dans le noir à la suite d'une cyberattaque d'une ampleur inédite. Les Russes avaient été désignés comme en étant les auteurs, ce qu'ils avaient nié…[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 de formation, de sensibilisation ou d'audits 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Des pirates russes ont pénétré le réseau électrique américain | Le Devoir

Une nouvelle doctrine en matière de cybersécurité

Une nouvelle doctrine en matière de cybersécurité

Jean-Yves Le Drian, ministre de la Défense, a inauguré hier un nouveau bâtiment de 9 000 m2 au centre DGA maîtrise de l'information à Bruz, près de Rennes. À cette occasion, il a dévoilé les grandes lignes de la nouvelle doctrine cyber des armées françaises. Elle reposera sur trois piliers : le renseignement, la protection/défense et la lutte informatique offensive.

« **L'irruption du numérique dans toutes les activités de la vie quotidienne nous oblige à repenser en profondeur l'art de la guerre.** » Hier, à Bruz, au sud de Rennes, dans les locaux de DGA maîtrise de l'information, « **le cœur battant du ministère de la Défense** », Jean-Yves Le Drian a présenté les grandes lignes de la nouvelle doctrine cyber des armées françaises.

Des combattants numériques

Cette doctrine s'appuiera sur trois piliers, a expliqué le ministre de la Défense. D'abord le renseignement, « **pour détecter les actions hostiles et leurs auteurs.** ». Ensuite, la protection et la défense : « **Nous devons bâtir d'épaisses murailles numériques.** » Enfin, la lutte informatique offensive : « **Nous avons besoin de combattants numériques pour riposter et neutraliser les cyber agresseurs.** »

Jean-Yves Le Drian a annoncé la création, en janvier 2017, d'un commandement français des opérations cyber (le « **CyberCom** »), placé sous la responsabilité directe du chef d'état-major des armées.

Ministre de la Cyberdéfense

C'est donc un Jean-Yves Le Drian, « **ministre de la Cyberdéfense** »,qui a passé la journée de lundi en Bretagne. Il a commencé par inaugurer officiellement le Pôle d'excellence cyber à Rennes. Cette association regroupe les chercheurs, les écoles et universités, les entreprises, les collectivités et les industriels qui œuvrent dans le numérique, la cybersécurité et la cyberdéfense.

Deuxième inauguration, un peu plus tard, dans les locaux de la DGA (direction générale de l'armement), à Bruz, au sud de Rennes. C'est ici que sont mis au point tous les systèmes d'information et de communication et les équipements électroniques des forces armées.

Le bâtiment baptisé Louis Pouzin – du nom d'un ingénieur français, précurseur d'Internet – est un bâtiment « **de haute qualité cyber** » qui accueille 270 experts sur 9 000 m2. Il est équipé de plus de 7 000 capteurs de sécurité, de 4 000 prises de réseau, dont 2 000 en fibre optique, le tout enveloppé dans 7 000 m3 de béton. Ici, des ingénieurs travaillent, entre autres, à détecter et à mettre hors d'état de nuire, les ennemis qui veulent capter les conversations téléphoniques des personnalités françaises, ou qui entendent prendra la main, à distance, sur la conduite des véhicules…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Drian annonce une nouvelle doctrine en matière de cybersécurité