La France dans le Top 10 du piratage informatique

La France dans le Top 10 du piratage informatique

NATIC Magazine vous fait une synthèse de l'actualité tournant autour des problématiques de cybersociété: Hacking, Sécurité, Codes malveillants, Piratage, Vie privée numérique, Protocole d'alerte, Alerte propagande, Web Tv, etc.

Le rapport annuel de Symantec sur le piratage informatique est une fois encore percutant. Selon le géant mondial de la cybersécurité, la France fait partie des 10 pays les plus concernés par les attaques informatiques. En 9ème position mondiale, le pays subit plus de 10 millions de tentatives avérées par an, en forte hausse d'une année sur l'autre.
Selon la version 2016 du rapport, les brevets technologiques et les trésors de propriété intellectuelle des grands groupes français attirent les meilleurs pirates mondiaux. Lancées par des concurrents, des activistes ou même des états, ces attaques visent également des PME ou même des particuliers ce qui est plus étonnant. Ces derniers sont très vulnérables notamment lorsqu'ils utilisent les réseaux sociaux. On observe en particulier une percée remarquable de l'utilisation des ransomwares ou rançongiciels – en hausse de 260% en France en 2015. Le phénomène prend de l'ampleur.
Dans le rapport de Symantec version 2016, le Top 3 des pays victimes de piratage en 2015 est constitué de la Chine, des Etats-Unis et de l'Inde.
Article original

Réagissez à cet article

Original de l’article mis en page : La France dans le Top 10 du piratage

---

Sensibilisation au Phishing

Sensibilisation au Phishing

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

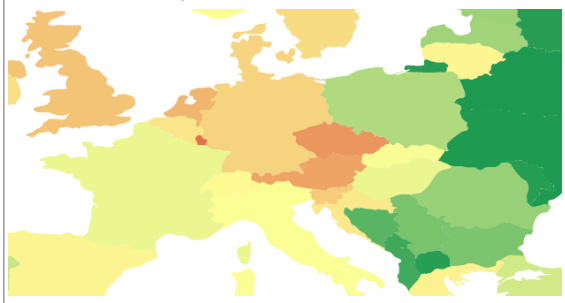
Contactez-nous

Réagissez à cet article

ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l’Europe

ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l’Europe

Les rapports de détection réalisés par ESET montrent une augmentation importante de la prolifération du malware JS/Danger.ScriptAttachement dans plusieurs pays européens. Les pays les plus touchés sont le Luxembourg (67 %), la République tchèque (60%), l'Autriche (57%), les Pays-Bas (54%) et le Royaume-Uni (51%).



ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l'Europe Les rapports de détection réalisés par ESET montrent une augmentation importante de la prolifération du malware JS/Danger.ScriptAttachement dans plusieurs pays européens. Les pays les plus touchés sont le Luxembourg (67 %), la République tchèque (60%), l'Autriche (57%), les Pays-Bas (54%) et le Royaume-Uni (51%).

ESET considère les ransomwares comme l'une des menaces informatiques les plus dangereuses à l'heure actuelle. Par conséquent, nous recommandons aux particuliers et aux entreprises de garder leurs ordinateurs et leurs logiciels à jour, d'utiliser un logiciel de sécurité fiable et de sauvegarder régulièrement leurs données importantes.

«Les utilisateurs d'ESET sont protégés contre cette menace. Nos solutions sont capables de bloquer le téléchargement et l'exécution en force par les différentes familles de ransomwares», commente Ondrej Kubovič, ESET IT Security Specialist.
En effet, lors du test réalisé par SE Labs qui compare 8 solutions de protection anti-malware, ESET Smart Security 9 remporte la première place avec 100% de réussite dans toutes les catégories.
«Chez ESET, nous nous engageons dans notre travail pour faire des produits qui protègent des millions d'utilisateurs à travers le monde. Nous apprécions de voir que les tests réalisés par SE Labs valident l'approche multicouches que nous construisons depuis plus de 20 ans.», a déclaré Palo Luka, Chief Technology Officer chez ESET.
ESET Smart Security 9 se distingue comme le seul produit ayant bloqué toutes les menaces. «ESET Smart Security contrôle parfaitement les attaques ciblées et les menaces Internet, ce qui est un excellent résultat. Il est rare d'obtenir 100% de réussite dans les tests de détection de menaces en temps réel, pour un produit sans compromis qui offre une protection complète et qui contrôle également des applications et des sites Web dits légitimes sans commettre une seule erreur», explique Simon Edwards, SE Labs' founder and Director.

Pour en savoir plus ces produits, rendez-vous sur http://www.eset.com/fr/
Article original de Benoit Grunemwald

Réagissez à cet article

Original de l'article mis en page : Locky se propage en Europe

---

Les dirigeants sont les

premiers responsables en cas de cyberattaques subies par leur entreprise

	**Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise**

Les dirigeants sont premiers responsables cas cyberattaques subies entreprise

Près d'un tiers (29 %) des responsables informatiques et près d'un cinquième (21 %) des employés en France considèrent donc que leur dirigeant devrait être tenu responsable en cas d'importante fuite de données. Pourtant, un quart (25%) des responsables informatiques admet ne pas informer son dirigeant en cas d'incident de ce type. Ce manque de transparence prive donc les dirigeants, considérés comme principaux responsables, d'une visibilité réelle sur les risques que représentent les fuites de données pour leur entreprise.

L'ampleur de ce constat est encore plus frappante dans une autre enquête menée par l'Economist Intelligence Unit pour le compte de VMware en début d'année. Celle-ci révélait en effet que seuls 8 % des dirigeants d'entreprises dans la région EMEA (11% en France) considéraient la cybersécurité comme une priorité. Alors que les cyberattaques s'intensifient et deviennent de plus en plus préjudiciables pour les entreprises – avec à la clé le risque de perte de propriété intellectuelle, de positionnement concurrentiel, et de données clients – l'impact sur la performance et l'image de marque peut être considérable.

Une nouvelle approche de la sécurité s'impose

Les entreprises sont de plus en plus menacées par de graves cyberattaques : plus d'un tiers (37 %) des répondants dans la région EMEA (seulement 28 % en France) s'attendent à en être victimes dans les 3 prochains mois. Malheureusement, les approches de sécurité actuelles ne sont pas adaptées à un monde toujours plus tourné vers les technologies numériques. Ainsi, plus d'un responsable informatique français sur trois (35 %) estime que l'un des principaux risques pour son organisation réside dans le fait que les menaces évoluent plus vite que les systèmes de défense mis en place.

« Le fossé entre dirigeants et responsables informatiques est symptomatique. Il symbolise le défi que doivent relever les entreprises cherchant à repousser leurs limites, à se transformer, à se différencier et à se protéger de menaces en constante évolution », déclare Sylvain Cazard, directeur général de VMware France. *« Aujourd'hui, les organisations les plus performantes sont celles qui sont capables de réagir rapidement et de préserver aussi bien leur image de marque que la confiance de leurs clients. Les applications et données des utilisateurs étant présentes sur un nombre d'appareils sans précédent, ces entreprises ont abandonné les approches traditionnelles de sécurité informatique incapables de protéger les entreprises numériques d'aujourd'hui. »*

Les employés et les processus aussi problématiques que les technologies

L'un des principaux risques pour la sécurité d'une entreprise provient de l'intérieur. Ainsi, pour 45 % des responsables informatiques de la région EMEA (et 37 % en France), la négligence ou le manque de formation des employés en matière de cybersécurité représente le principal défi pour leur entreprise. L'enquête montre également jusqu'où les salariés sont prêts à aller pour accroître leur productivité : 15 % d'entre eux (contre 21% au niveau EMEA) utilisent leurs appareils personnels pour accéder à des données professionnelles, tandis que 14 % (17% en EMEA) sont prêts à enfreindre la politique de sécurité de leur entreprise afin de travailler plus efficacement.

« La sécurité n'est pas qu'une question de technologie. Comme le montrent les résultats de notre enquête, les décisions et les comportements des employés ont également un impact sur l'intégrité d'une entreprise » remarque Sylvain Cazard. *« Malgré tout, la solution n'est pas non plus de tout verrouiller et d'instaurer une culture de la peur. Les organisations qui adoptent des approches intelligentes proposent plus de moyens et non de restrictions à leurs employés, leur permettant de s'épanouir, d'adapter les process et de transformer leur activité pour réussir.»*

« Les entreprises tournées vers l'avenir sont conscientes du fait que les stratégies de sécurité réactives d'aujourd'hui ne sont plus efficaces pour protéger leurs applications et données. Adopter une approche software-defined garantissant l'omniprésence de la sécurité leur offre la flexibilité nécessaire pour réussir en tant qu'entreprises numériques », conclut Sylvain Cazard.

Réagissez à cet article

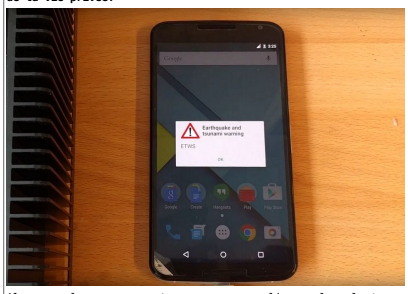
Original de l’article mis en page : Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

---

Appli alerte attentats : «Il faut que la France respecte les standards internationaux»

	**Application Alerte Attentats : «Il faut que la France respecte les standards internationaux»**

Alors que le gouvernement propose une application pour les alertes aux attentats, Gaël Musquet, hacker et militant du logiciel libre, presse l'Etat d'adopter la diffusion cellulaire, plus efficace et respectueuse de la vie privée.



Alors que le gouvernement propose une appli pour les alertes aux attentats, Gaël Musquet, hacker et militant du logiciel libre, presse l'Etat d'adopter la diffusion cellulaire, plus efficace et respectueuse de la vie privée.
Le gouvernement a dévoilé mercredi une application, «SAIP» (pour «Système d'alerte et d'information des populations»), permettant d'alerter en direct ses utilisateurs en cas d'attentat à proximité. Une bonne initiative, mais une réponse technologique inappropriée, estime Gaël Musquet, hacker en résidence à la Fonderie, l'Agence numérique publique d'Ile-de-France. Car des normes internationales existent déjà pour transmettre une alerte sur tous les téléphones des populations menacées par un risque, sans qu'elles aient besoin d'installer une application, et en respectant leur vie privée.

Que penser de cette application d'alerte gouvernementale ?
Prévoir un protocole d'alerte aux populations est une bonne initiative, on va dans le bon sens. Nous n'avons pas une grande culture du risque en France, donc toutes les occasions d'en parler sont bonnes à prendre ! Cela permet de faire de la pédagogie, d'informer et de former les populations. Car c'est le manque de préparation qui crée de la panique, et malheureusement, parfois des morts. Et puis franchement, les sirènes d'alerte ne sont comprises par personne, donc il est temps de rafraîchir le système avec un peu de technologie.
Le taux d'équipement en smartphones permet aujourd'hui de toucher un maximum de personnes quand on développe une application sur les deux principales plateformes, iOS et Android. Le gouvernement a eu une démarche d'ouverture, en consultant par exemple Visov, une association de volontaires spécialistes de la gestion d'urgence – ils font de la pédagogie auprès des pompiers, des gendarmes ou de l'Etat, entre autres, sur l'utilisation du Web et des réseaux sociaux en cas de crise. Le développement de SAIP est encore en cours, et il appartient au Service d'information du gouvernement [SIG] de recueillir les premiers retours pour améliorer le service. Il a fait cette application de la manière la plus agile possible, on ne peut pas lui faire de reproche là-dessus.

Mais… ?
Il y a plusieurs problèmes avec cette démarche. D'abord, l'application SAIP s'appuie sur les données internet des smartphones, donc sur les réseaux 3G, 4G et wifi qui sont potentiellement vulnérables. Quand il y a trop de téléphones dans une certaine zone et pas assez de canaux disponibles pour pouvoir router tous les appels, les antennes-relais sont saturées et elles ne peuvent plus répondre. Ça se passe régulièrement dans les événements où il y a foule : pendant les attentats de Boston, au discours d'investiture d'Obama mais aussi le 13 Novembre, il y a eu ce qu'on appelle un Mass Call Event (MCE). C'est aussi le cas localement dans des quartiers à cause de concerts, festivals… Quand on sait à l'avance qu'il y aura trop d'appels durant un événement, on installe des antennes-relais supplémentaires pour couvrir le risque de saturation. C'est ce qui va se passer pour l'Euro de foot. Mais en cas de crise imprévue, les infrastructures ne résisteront pas, ni pour les appels, ni pour les SMS, ni pour les données internet. Ce sont des lois physiques, on ne peut rien y faire. Dans ce genre de situation, SAIP sera dans les choux.
Ensuite, il faut faire attention à ne pas morceler le système d'alerte avec de multiples applications de gestion de crise. Il existe une appli pour le risque d'attentats en France, une pour les séismes du Centre sismologique euroméditerranéen, une autre pour mes vacances en Russie et une pour les alertes de l'Indre-et-Loire… Il y a aussi des entreprises privées qui développent leurs propres applications d'alerte, et des fois, comme pour les risques d'avalanches, elles sont meilleures que celles de l'Etat. La concurrence entre les acteurs est contre-productive pour toucher un maximum de personnes. Il vaut mieux un système universel qui puisse aussi s'adresser, par ailleurs, aux touristes de passage en France.
Enfin, il y a la question du respect de la vie privée. Beaucoup d'internautes s'inquiètent déjà, sur Twitter, que l'Etat puisse savoir en permanence où je me trouve via les données de géolocalisation récoltées par cette application. Et il existe effectivement un risque que ces données soient piratées, quels que soient les efforts de sécurisation. Et puis, comme ce n'est pas un logiciel libre, on ne connaît pas son code source et la communauté des développeurs ne peut pas aider à corriger les bugs, faire des stress tests pour vérifier son fonctionnement dans des conditions d'usage intense…

Y a-t-il une meilleure solution ?
A court terme, c'est bien d'avoir une application d'alerte. Mais à long terme, on n'y coupera pas : il faut que la France respecte les standards internationaux de la diffusion cellulaire – cell broadcast en anglais. C'est une norme qui existe déjà pour la diffusion des alertes, et qui permet d'informer toutes les personnes présentes dans la zone de couverture d'une antenne-relais. On n'a pas besoin de connaître leur numéro de téléphone ni de leur faire installer une application : dans la région prédéfinie, tout le monde sans exception reçoit le SMS, y compris les touristes avec un forfait étranger ! C'est une technologie non intrusive qui respecte la vie privée des citoyens. Elle ne se limite pas aux possesseurs d'iPhone et d'Android, même pas besoin d'avoir un smartphone : l'alerte arrive même sur les petits téléphones. Ça tombe bien : en France, 92 % des personnes de plus de 12 ans ont un téléphone, mais 58 % seulement ont un smartphone. Et puis la norme cell broadcast prévoit que les messages d'alerte passent au-dessus de la mêlée dans le trafic téléphonique.

Simulation d'une alerte en diffusion cellulaire sur Android.

La norme du cell broadcast est définie depuis 1995 (pdf et pdf). Elle a même été testée à Paris en 1997 : tout est déjà là ! Depuis, elle a évolué pour supporter les alertes enlèvement (Amber), les séismes et les tsunamis (système ETWS). Avec l'arrivée de la 4G, le protocole a encore été étendu et on peut même l'utiliser pour diffuser des vidéos, aujourd'hui. Vingt ans plus tard, la diffusion cellulaire a été déployée par nos voisins – Espagne, Portugal, Italie, Finlande, Pays-Bas, Chine, Etats-Unis, Israël… Et la France brille par son absence.
Nous devons, nous aussi, la mettre en place dans le cadre d'une véritable politique numérique de l'alerte. Il y a là un enjeu de sécurité publique. Cette norme doit être imposée à nos opérateurs téléphoniques, comme un service public de l'alerte, comme on a imposé la mise en place du 112. C'est une question d'intérêt général. Pourquoi ne respectons-nous pas les normes et standards internationaux en matière d'alerte, documentés, ouverts et qui ont fait leurs preuves ?

Pourquoi n'a-t-on pas encore déployé la diffusion cellulaire en France ?
C'est fragile et ça coûte cher, nous dit-on. Oui, ça coûte cher, mais pas plus que la Hadopi ! On a su débloquer des budgets pour les lobbys de l'industrie culturelle et créer, entretenir, maintenir l'Hadopi à grands frais en contraignant les opérateurs à suivre. Idem pour l'espionnage de masse avec les lois sur la surveillance. Si tu es capable de m'espionner, alors tu es capable de m'informer en cas de crise. Est-ce que notre sécurité vaut moins que les doléances d'autres lobbys ? Nos vies sont-elles moins chères que la Hadopi ?
La mise en place du cell broadcast demande effectivement, quoique pas obligatoirement, de légiférer. Ça demande ensuite que les systèmes d'information des préfectures soient reliés aux systèmes d'information des opérateurs téléphoniques : il faut des passerelles pour que l'alerte passe de la préfecture à SFR, Bouygues et compagnie. Ça demande de la réflexion et un chantier technique. A part ça, c'est simple : les antennes-relais respectent déjà la norme.

Simulation d'une alerte en diffusion cellulaire sur iPhone.

Il faut juste activer l'option. Nos voisins chiliens ont su le faire pour se protéger des tsunamis ; en septembre 2015, il leur a fallu quelques dizaines de minutes seulement pour évacuer des milliers de personnes après le séisme. Il n'y a pas de raison que la France n'y arrive pas aussi !

C'est une question plus générale de culture du risque…
L'alerte est une chose, oui, mais ce n'est pas suffisant. La France est un pays qui fait face à tous les risques possibles, mais nous n'avons pas de culture du risque. Alors que les risques, eux, sont bien là. Notre mémoire est courte mais nous avons des catastrophes naturelles bien plus meurtrières que le terrorisme : 500 morts après la rupture du barrage de Malpasset en 1959, 46 morts avec le séisme provençal de 1909, 29 000 morts pour l'éruption en 1902 de la Montagne Pelée, 70 000 morts dans le tsunami de 1908 à Messine, et même 29 morts récemment à La Faute-sur-Mer et 17 morts dans les inondations de la Côte d'Azur en octobre 2015.
Il faut faire des exercices : un barrage a lâché, que fait-on ensuite ? Les gens paniquent quand ils ne savent pas quoi faire, on l'a encore vu la semaine dernière avec les crues. Il faut des exercices communaux pour expliquer les procédures aux habitants des villes, former des gens à l'utilisation des réseaux sociaux en cas d'urgence pour contrer les rumeurs et diffuser les informations, former des pilotes de drones et des radioamateurs : le jour où il y a un vrai black-out de téléphonie, qui saura faire la transmission des informations ? Au-delà d'événements très médiatiques comme les hackathons ou les simulations entre experts, nous devons impliquer la société civile dans des exercices réguliers.
Commençons à expérimenter sur des territoires français de petite taille, en proie à des crises cycliques – Guadeloupe, Martinique, Réunion, Polynésie… Des formats d'événements existent déjà. CaribeWave, IndianWave et PacificWave sont par exemple des exercices annuels d'alerte au tsunami, auxquels je participe. Les Etats-Unis organisent un «préparathon» contre les catastrophes naturelles.

2016 est l'année de la présidence française de l'Open Governement Partnership. Pour un gouvernement ouvert, à nous, société civile, de nous prendre en charge, nous investir dans les exercices et les réflexions pour une meilleure information et une meilleure préparation aux crises.
Vendredi après-midi, tout le matériel technologique ayant servi à CaribeWaveFWI, la dernière simulation d'alerte au tsunami, sera exposé à la Gaîté Lyrique à Paris, dans le cadre du festival Futurs en Seine.

Article original de Camille Gévaudan

Réagissez à cet article

Original de l’article mis en page : Appli alerte attentats : «Il faut que la France respecte les standards internationaux» – Libération

---

Hardwear.io 2016 : Hardware Security Conference

Hardwear.io 2016 : Hardware Security Conference

Les 22 et 23 septembre 2016, à La Hague (Pays-bas) la seconde édition de la Hardwear.io se penchera sur la sécurité des objets connectés.

hardwear.io
Hardware Security Conference and Training

A l'ère de l'automatisation où la technologie joue un rôle clé dans l'amélioration de l'efficacité des dispositifs, la nécessité de traiter de manière proactive la sécurité matérielle est largement sous-estimée. Allant de simples gadgets connectés utilisés au quotidien, aux systèmes automobiles, aux appareils médicaux sans fil où au matériel de défense nationale ; tout fonctionne sur une technologie sophistiquée mais très vulnérable .
Hardwear.io propose à la fois une plate-forme et une communauté, une occasion d'échanger entre professionnels, et le plus important apporte des solutions aux problèmes critiques relatifs à la sécurité du hardware.
Des sessions de formation se tiendront pendant deux jours, avant la tenue de la conférence, les 20 et 21 septembre 2016 à la Hague, aux Pays-bas. Avec des intervenants de renom, pour échanger sur divers sujets comme les backdoors, l'exploitation des failles, la confiance, les assurances et les attaques sur l'équipement matériel, les firmware et protocoles connexes .
Hardwear.io est est menée par l'équipe de nullcon – Conférence internationale de sécurité basée en Inde, l'un des événements de la sécurité des systèmes d'information de premier plan en Asie depuis 2010. Hardwear.io est une conférence qui apporte à la fois une plate-forme et une communauté pour la sécurité du matériel informatique, où les chercheurs mettent en valeur leurs travaux et échangent leurs innovations liées aux attaques et à la défense hardware. L'objectif de la conférence tourne autour de quatre principales préoccupations : le firmware et les protocoles connexes à savoir backdoors, exploits, la confiance et les attaques.

L'APPEL A CONTRIBUTIONS EST OUVERT
Pour tous ceux qui souhaitent intervenir lors de la conférence Hardwear.io 2016, les sujets peuvent être soumis jusqu'au 5 juillet 2016 via hardwear.io. Hardwear.io privilégie les sujets ayant trait à la sécurité du matériel en profondeur, à la fois sous l'angle offensif et défensif.

Parmi les domaines proposés (sans s'y limiter) :
– Circuits intégrés
– Processeurs
– Internet des objets / Smart Devices
– Crypto Hardware
– Systems embarqués
– Systèlmes automatisés Automobile, Aerien, train et composants hardware
– Systèmes de controle industriels / SCADA
– Systèmes Satellites
– Objets médicaux connectés
– Smartphone firmware, hardware
– Firmware
– Test de pénétration Hardware
– Module plateforme de confiance
– Protocoles de communication Radio et hardware
– Confiance et assurance Hardware et algorithms
– Multimedia hardware, firmware, protocols
– Telecom Hardware et réseaux
– Serrures éléctroniques et physiques
Parmi les intervenants clés en 2015, Hardwear.io a accueilli : Jon Callas, Harald Welte, Javier Vidal, Jaya Baloo, Florian Grunow et d'autres experts de renom en sécurité qui ont tous renforcé l'équipe des organisateurs de la nécessité de poursuivre ces rencontres de la sécurité hardware dans le monde ultra connecté d'aujourd'hui. Pour plus d'information, et pré-ventes early bird: http://hardwear.io
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Hardwear.io 2016 : Hardware Security Conference – ZATAZ

L’investigation pour recouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

L’investigation pour recouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.

L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.

L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel.
Article original de Balázs Scheidler

Réagissez à cet article

Original de l'article mis en page : Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse

---

Code de la communication – La loi contre la

cybercriminalité à réviser

	Code de la communication – La loi contre la cybercriminalité à révise

Les internautes et les utilisateurs des réseaux sociaux espèrent que le projet de code de la communication a abrogé l'article 20 de la loi sur la lutte contre la cybercriminalité. Le gouvernement tiendra-t-il une promesse faite en 2014 ?

Le gouvernement tiendra-t-il les promesses faites par ses anciens membres ? La révision, voire l'abrogation de l'article 20 de la loi sur la lutte contre la cybercriminalité, fait partie des dispositions les plus attendues du projet de code de la communication. Adopté jeudi en conseil des ministres, et attendu incessamment devant les bureaux du Parlement, le projet reste, pour l'instant, inaccessible. Le sort de l'article 20 de la loi contre la cybercriminalité qui avait été abrogé dans l'avant-projet de texte soumis au gouvernement demeure encore inconnu.

Le président de la République ayant déjà affiché sa volonté de supprimer les peines de prison pour sanctionner certains délits de presse comme les injures ou la diffamation, on voit mal comment le Conseil des ministres aurait pu enlever du projet la disposition finale qui a indiqué, entre autres, l'abrogation du fameux article 20. Sanctionnant de peine de prison pouvant aller jusqu'à cinq ans, et d'amende pouvant s'élever jusqu'à 100 millions d'Ariary, toute personne coupable d'injures, de diffamation ou d'atteinte à la dignité d'une personne, par le biais de tout type de support, écrit, audio-visuel ou électronique, le fameux article 20 a soulevé un tollé aussi bien dans le milieu de la presse que parmi les utilisateurs des réseaux sociaux.

La ministre de la Justice et celui de la Communication de l'époque, pour calmer les esprits, avaient alors promis que des ajustements pourraient être apportés au texte s'il devait se trouver en contradiction avec le code de la Communication qui était alors en cours d'élaboration.

Or, en instituant les peines de prison et les amendes exorbitantes pour toute diffamation ou injure faite par voie électronique, la loi, sur la lutte contre la cybercriminalité est entrée en contradiction avec l'esprit qui avait guidé l'élaboration du Code de la communication.

Risque de maintien

De l'eau a, pourtant, coulé sous le pont depuis la validation du texte par le monde médiatique. Vu les relations de la présidence avec les internautes, notamment les utilisateurs du réseau social Facebook, il n'est pas impossible que les autorités aient préféré laisser tel quel l'article 20 de la loi sur la lutte contre la cybercriminalité. L'objectif étant que, comme l'aiment le dire les responsables de la communication des autorités, « limiter le confort de l'internaute qui se trouve devant son clavier et qui se croit intouchable ».

Certaines sources laissent par ailleurs entendre que durant ce long intervalle de temps entre la validation de l'avant-projet et son adoption en conseil des ministres, l'Exécutif a trouvé le temps de réintégrer les dispositions qui avaient été jugées liberticides par les professionnels des médias, et de retirer les articles plus « libéraux », tel que celui qui a abrogé l'article 20 de la loi contre la cybercriminalité. Il semblerait même que le texte, dans une de ses versions manipulées par le Gouvernement, fasse référence à cet article 20 en indiquant que certaines peines seront appliquées sans préjudice de celles prévues par la loi sur la lutte contre la cybercriminalité.

Attendue depuis sa promulgation en 2014, la révision de la loi sur la lutte contre la cybercriminalité, notamment en ce qui concerne l'abrogation de son article 20, pourrait finalement être une réalité maintenant que le code de la communication est en passe d'être adopté. Tout comme la fameuse loi peut encore rester telle une épée de Damoclès suspendue au-dessus de la tête des professionnels des médias, mais aussi des internautes et des utilisateurs des réseaux sociaux.

Réagissez à cet article

Original de l’article mis en page : Code de la communication – La loi contre la cybercriminalité à réviser | LExpress de Madagascar – Actualités en direct sur Madagascar

---

Piratage d’utilisateurs de TeamViewer : utilisateurs négligeants ?

Piratage d’utilisateurs de TeamViewer : utilisateurs négligeants ?

Un nombre conséquent d'utilisateurs de TeamViewer se sont plaints du piratage de leur compte. La société américaine indique que les utilisateurs sont responsables… de leur négligence.

De nombreuses sociétés Internet comme Reddit ont dû modifier les mots de passe de certains de leurs utilisateurs, 100.000 pour Reddit, à la suite du piratage massif des données de Myspace, LinkedIn… Pourquoi ? Les utilisateurs exploitaient le même mot de passe sur différents supports numériques. Autant dire du pain béni pour les pirates. Parmi les victimes, le fondateur de Facebook. Lui, il cherchait doublement les ennuis, son mot de passe n'était rien d'autre que « dadada« . Bref, à force de penser que cela n'arrive qu'aux autres, le danger vous tombera dessus, un jour ou l'autre, et plus rapidement que vous pourriez le penser.
TeamViewer, l'outil qui permet de se connecter sur un ordinateur, à distance, vient d'alerter ses utilisateurs. Un grand nombre de clients TeamViewer s'étaient plaints du piratage de leur compte. L'entreprise a utilisé le terme de « négligence » pour définir les récents problèmes.
TeamViewer a mis en place, la semaine dernière, un nouveau système de sécurité pour renforcer les connexions : la double authentification. Le porte-parole de TeamViewer a indiqué que le développement des outils de sécurité avait commencé, il y a quelques semaines, lorsque les premiers rapports de vols de compte ont émergé du web.

Article original de Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Piratage dutilisateurs de TeamViewer : la faute aux utilisateurs – Data Security BreachData Security Breach

---

Cloud souverain : les collectivités locales ne pourront pas y couper

Cloud souverain : les collectivités locales ne pourront pas y couper

Dans une circulaire publiée au Journal Officiel, le Ministère de la Culture indique que les collectivités locales françaises devront passer par des prestataires hébergés en France pour traiter les données relatives aux citoyens français.

Mieux vaut tard que jamais : une circulaire parue au Journal officiel et signée par la direction générale des collectivités locales et le service interministériel des Archives de France vient clarifier les dispositions relatives au « cloud souverain ». Le texte, repérée par NextInpact, explique que les collectivités françaises devront impérativement passer par des prestataires situés sur le territoire français pour stocker et traiter les données dans le cloud.

Le texte se veut une clarification des directives données dans le cadre du « Guide sur le cloud computing et les datacenters à l'attention des collectivités locales. » La circulaire précise notamment le statut des données produites par les collectivités territoriales. Celles-ci « relèvent du régime politique des archives publiques dès leur création. ».

Point de salut

Outre cet aspect, la circulaire précise quelques lignes plus loin que « toutes les archives publiques sont par ailleurs des trésors nationaux en raison en raison de l'intérêt historique qu'elles présentent ou sont susceptibles de présenter. » Un régime qui s'applique autant aux documents physiques qu'à leurs équivalents numériques et qui implique une nécessaire localisation des données sur le territoire national. Celle-ci ne peut être contournée qu'à titre temporaire sur une demande adressée directement au ministère de la Culture.

Hors des fournisseurs de cloud souverain, point de salut pour les collectivités qui souhaitent avoir recours à ce type de service. La circulaire donne également une définition de ce que l'administration entend par cloud « souverain » : un « cloud dont les données sont entièrement stockées et traitées sur le territoire français. » La circulaire précise également que l'Anssi travaille sur la production d'une offre de labellisation des offres qui répondent à ces critères, label baptisé « Secure Cloud ».

Initié en 2014, le label n'est pas encore entièrement opérationnel et est encore en « phase d'expérimentation » jusqu'à la moitié de l'année 2016 selon le site de l'Afnor. Celui-ci devrait donc sous peu être en mesure de proposer une liste de fournisseurs qualifiés pour répondre aux besoins des collectivités locales en matière de services cloud.

Article original de ZDNet

Réagissez à cet article

Original de l’article mis en page : Cloud souverain : les collectivités locales ne pourront pas y couper – ZDNet