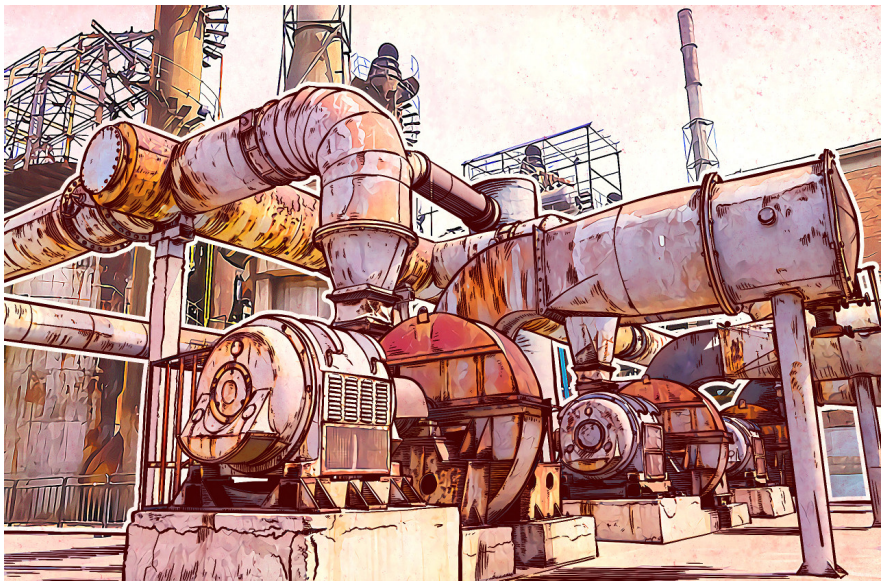
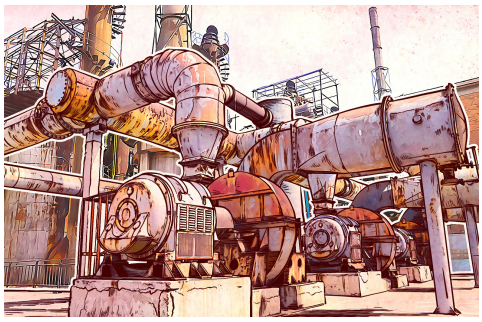
Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie



Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

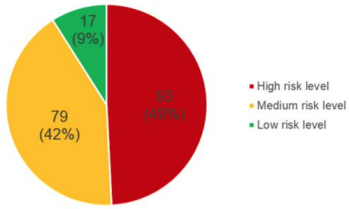
On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Quand les pirates s’attaquent à l’éducation

	Quand les pirates s’attaquent à l’éducation

---

Le milieu scolaire n'est pas épargné par les hackers, certains étudiants piratent les examens, les notes ou leurs professeurs, tirant profit d'outils prêts à l'emploi mais aussi d'un manque de moyens et de sensibilisation des principaux concernés.

De nombreux collèges, écoles ou lycées sont les cibles de cyber-attaques perpétrées par des étudiants. Des offensives qui : *«sont réalisées par des digital natives, des jeunes à l'aise avec l'informatique qui sont nés avec un ordinateur entre les mains»*, explique Jean-Charles Labbat, directeur général France, Belgique, Luxembourg et Afrique francophone chez Radware, société spécialisée en sécurité informatique.

Des attaques basiques

Trois secteurs sont principalement visés par ces hacks : les examens, les notes, puis les systèmes informatiques des institutions ou des professeurs. Et les méthodes utilisées ne sont pas des plus sophistiquées.
Un étudiant pas suffisamment préparé pour passer un examen (comme les QCM en ligne dans certains pays) peut essayer de bloquer le site. Pour ce faire, il utilise le déni de service, il se connecte à ce serveur et se rend au point de connexion pour y envoyer une surcharge d'informations et boucher l'accès à l'application. Un hack très simple puisque, comme l'explique Jean-Charles Labbat, *« des outils sont disponibles sur internet comme Slowloris, ou il suffit de rentrer l'adresse du serveur pour le faire tomber ».*
Pour les systèmes de notation, rien de bien compliqué non plus. Les notes sont rangées dans une base de données et pour consulter ses résultats il faut se connecter avec ses identifiants. Le pirate va recourir à une injection SQL pour rentrer sans mot de passe, accéder directement à la base de données et modifier les informations renseignées. En novembre 2014, un élève du Tarn avait augmenté sa moyenne la faisant passer de 8,76 à 10,62.
Les enseignants sont également ciblés, via l'envoi de spams par exemple. *« Les enseignants recourent de plus en plus à l'outil informatique pour leurs cours. Un étudiant malveillant peut très bien s'il le souhaite accéder à un ordinateur mal protégé, spammer son professeur mais aussi ses contacts ou affecter tout le réseau de l'école* »...[lire la suite]

Denis JACOPINI est **Expert Informatique assermenté et formateur** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles

---

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 : Quand les pirates s’attaquent à l’éducation > Mag-Securs

Une garantie d’un million de dollars contre les ransomwares

Une garantie d’un million de dollars contre les ransomwares

Un éditeur de logiciels de cybersécurité propose de reverser jusqu'à un million de dollars à ses clients qui seraient, malgré ses protections, victimes d'un virus informatique.

Ce n'est pas une incitation à payer les rançonneurs informatiques. Hier, l'éditeur de logiciels de cybersécurité SentinelOne a annoncé proposer à ses clients professionnels une garanti d'un montant maximum d'un million de dollars contre toute menace qui percerait ses défenses. Notamment les ransomwares, ses programmes malveillants qui coupent l'accès aux données stockées dans les ordinateurs touchés et invitent à payer pour les récupérer. La police conseille de ne jamais céder à ce chantage.
SentinelOne compte sur sa technologie de machine learning pour protéger ses clients. En cas de manquement à ses devoirs, l'éditeur dédommagerait les entreprises à hauteur de 1.000 dollars par postes de travail et dans la limite d'un million de dollars. « *Avec cette assurance financière, nous devenons vraiment responsables de la sécurité de nos clients*, souligne Scott Gainey, le patron du marketing de SentinelOne,*jusqu'ici, les entreprises victimes qui voulaient se retourner contre leurs éditeurs d'anti-virus ne pouvaient pas, c'est injuste*. » D'après lui, cette garantie est une première au monde…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : Une garantie d'un million de dollars contre les ransomwares, Cybersécurité — Les Echos Business

Sécurité informatique des collectivités : Toujours plus avec moins…

Sécurité informatique des collectivités : Toujours plus avec moins…

Les collectivités et leurs groupements, notamment les communautés de communes, peinent encore à prendre en compte tous les aspects de la sécurité des systèmes d'information, à en croire le rapport 2016 du Club de la sécurité de l'information Français (Clusif). Alors qu'elles se numérisent de plus en plus, les collectivités vont devoir maintenir voire accentuer leurs efforts dans un contexte budgétairement contraint.

Dans l'édition 2016 de son rapport sur les « Menaces informatiques et pratiques de sécurité en France » (Mips), le Club de la sécurité de l'information Français (Clusif) se penche de nouveau sur les collectivités (1). De plus en plus nombreuses à recourir à des services dématérialisés, celles-ci auront à charge de « maintenir » leurs « efforts » pour « assurer la sécurité de leur système d'information et des informations qui leur sont confiées », selon les auteurs de ce document de plus de cent pages. Le tout dans un contexte budgétaire restreint. Globalement, alors que le sentiment de dépendance à l'égard du numérique s'enracine, la sécurité des systèmes d'information est « efficiente dès lors que les moyens organisationnels, humains et financiers sont clairement attribués » et que la direction est fortement impliquée, indique le rapport. Cependant, sur la base des 203 collectivités interrogées, il est fait état de grandes disparités entre les échelons territoriaux, où les communautés de communes sont à la peine.

Stagnation des budgets malgré la numérisation en cours

Publié tous les deux ans, le « Mips » délivre un bilan approfondi des usages en matière de sécurité de l'information ; et inclut dans son édition 2016 (comme tous les 4 ans) les collectivités territoriales de grande taille. Autrement dit les communes de plus de 30.000 habitants, les intercommunalités (communautés de communes, d'agglomération, communautés urbaines ou encore les métropoles) et enfin les régions et les départements (regroupés par le rapport sous le terme de conseils territoriaux).

Côté résultats, si une grande partie des collectivités interrogées a confié un sentiment toujours croissant de « dépendance » vis-à-vis de l'informatique (75% contre 68% en 2012), les budgets qui y sont liés tendent pourtant à baisser et restent très disparates (avec un rapport de 1 à 100 entre les plus petits et les plus importants). Ainsi, près de 54% des collectivités ont un budget informatique inférieur à 100.000 euros en 2016, contre 45% en 2012. En moyenne, les conseils territoriaux sont les mieux dotés avec 5,8 millions d'euros, pour un million d'euros dans les intercommunalités et 800.000 euros dans les villes.

Dans ce total, la part de la sécurité est difficilement évaluable et demeure au mieux constante (67% des cas) ou diminue (28% des collectivités contre 14% en 2012 y consacrent moins de 1% de leur budget informatique). Enfin, si augmentations il y a, elles servent avant tout à mettre en place des solutions de sécurité (25%), même si des efforts importants sont effectués en matière organisationnelle (11%) et en sensibilisation (9%).

Pas de politique de sécurité sans personnels qualifiés

Bien que majeur, l'aspect financier n'occupe que la deuxième place des principaux freins pour les collectivités (à 45%), pour qui l'absence de personnels qualifiés semble être le véritable problème (à 47%), accru par un manque avoué de connaissance (38%). En conséquence, les contraintes organisationnelles (29%) et les réticences de la direction générale, des métiers ou des utilisateurs (24%) ferment la marche.

Malgré tout, l'étude montre que les collectivités sont de plus en plus nombreuses à formaliser leur politique de sécurité (PSI), en particulier les villes (54% contre 43% en 2012) et les conseils territoriaux (52% contre 35%). A l'inverse, les communautés de communes sont à la peine (un peu plus de 2 sur 10).

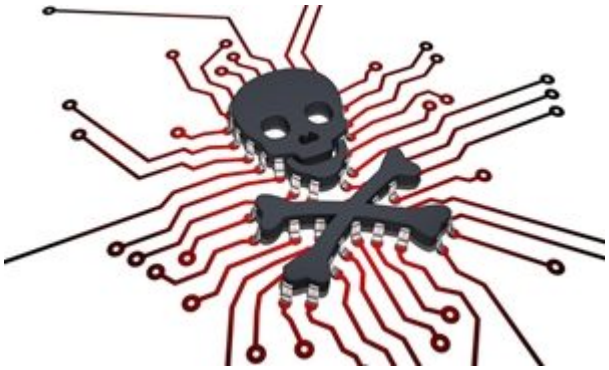
Concrètement, les DSI (directions des systèmes d'information) gèrent les politiques de sécurité dans 65% des cas, alors que les directions générales des services tendent à se désengager (impliquées dans 54% des cas, contre 80% en 2012). Dans 21% des cas, des élus y ont contribué. Enfin, on notera que la présence d'un responsable de la sécurité des systèmes d'information (RSSI) « serait une condition sine qua none pour disposer d'une PSI ». Par ailleurs de plus en plus nombreux (+3 points, à 35%), les RSSI voient cependant leur fonction se diluer, avec 39% de personnel dédié en 2016 contre 62% en 2012 dans les villes, pour ne citer qu'elles. Enfin, ils sont bien souvent rattachés à la DGS (dans les communautés de communes notamment) ou à la DSI (dans les régions ou les départements par exemple) – selon une règle qui veut que « plus la collectivité est petite et plus les fonctions sont cumulées par le comité de direction »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Sécurité informatique : les collectivités encouragées à maintenir leurs efforts – Localtis.info – Caisse des Dépôts

---

Des serveurs Linux attaqués par le ransomware Fairware



Des serveurs Linux attaqués par le ransomware Fairware

Des exploitants de serveurs Linux signalent des attaques qui entraînent la disparition du dossier Internet du serveur et la non disponibilité des sites pendant une durée indéterminée.

Les participants aux forums de BleepingComputer se plaignent également de l'attaque : d'après la description fournie par une des victimes, cela ressemble plus à une attaque via force brute contre SSH. Notons qu'à chaque fois, le dossier Internet est supprimé et il ne reste que le fichier read_me qui contient un lien vers une page Pastebin où apparaît la demande de rançon.
Les individus malintentionnés promettent de rendre les fichiers contre 2 bitcoins et expliquent que le serveur de la victime a été infecté par le ransomware Fairware. Toutefois, à en croire Lawrence Abrams de chez Bleeping Computer, cette affirmation pourrait ne pas être tout à fait exacte.
« Si l'attaquant télécharge un programme ou un script pour réaliser « l'attaque », il s'agit alors bel et bien d'un [ransomware]. Malheureusement, nous ne disposons pas pour l'instant des informations suffisantes. Tous les rapports montrent que les serveurs ont été compromis, mais je n'ai pas encore eu l'occasion de le vérifier » a déclaré l'expert.
La demande de rançon contient l'adresse d'un portefeuille Bitcoin. La victime est invitée à réaliser le paiement dans les deux semaines, sans quoi les individus malintentionnés menacent d'écouler les fichiers sur le côté. Le message publié sur Pastebin possède le contenu suivant : « Nous sommes les seuls au monde qui pouvons vous rendre vos fichiers . Après l'attaque contre votre serveur, les fichiers ont été chiffrés et envoyés vers un serveur que nous contrôlons. »
Le message contient également une adresse email pour l'assistance technique, mais il est interdit à l'utilisateur d'y envoyer un message uniquement pour confirmer si les attaquants possèdent bien les fichiers perdus. Lawrence Abrams affirme que pour l'instant, il ne sait pas ce que les attaquants font avec les fichiers. Vu que les fichiers sont supprimés, il serait plus logique pour les conserver de les archiver et de les charger sur un serveur et non pas de les chiffrer et de gérer des clés individuelles.
En général, les ransomwares sont diffusés via l'exploitation de vulnérabilités ou par la victime elle-même qui est amenée, par la ruse, à exécuter le malware. Dans le cas qui nous occupe, rien ne trahit ce genre d'activité. Une des victimes indiquait sur le forum de Bleeping Computer que son serveur Linux avait été épargné en grande partie par l'attaque et que les fichiers de la base de données avaient été préservés. Ce commentaire indiquait également que les individus malintentionnés avaient laissé le fichier read_me dans le dossier racine.
La suppression de fichiers et le refus de confirmer leur vol sont des comportements inhabituels pour des individus malintentionnés qui travaillent avec des ransomwares. « Il est tout à fait possible qu'il s'agisse d'une escroquerie, mais dans ce cas c'est un mauvais business pour les attaquants » explique Lawrence Abrams. « Si l'escroc ne respecte pas sa promesse après le paiement de la rançon, il aura mauvaise réputation et plus personne ne le paiera. »
Toutefois, le message sur l'infection via le ransomware et la menace de publier les données volées sont en mesure de confondre la victime et de l'amener à répondre aux exigences des attaquants. Fairware n'est pas la première cybercampagne accompagnée d'une telle menace. L'année dernière, les exploitants du ransomware Chimera, avaient adopté une astuce similaire, même si leur malware n'était pas en mesure de voler les fichiers ou de les publier sur Internet.
Lawrence Abrams explique que les victimes de ransomwares devraient s'abstenir de payer la rançon, mais si elles décident d'agir ainsi, elles doivent au moins confirmer que le bénéficiaire du paiement possède bien les fichiers.
Article original de Securelist

Réagissez à cet article

Original de l’article mis en page : Fairware attaque des serveurs Linux – Securelist

---

Directive NIS adoptée: quelles conséquences pour les entreprises?

Directive NIS depuis juillet. Des changements pour les entreprises?

En juillet dernier, le Parlement européen a adopté la directive NIS (Network and Information Security). Les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.

C'est fait ! La directive NIS a été approuvée le 6 juillet par le Parlement européen en seconde lecture, après avoir été adoptée en mai dernier par le Conseil de l'Union européenne. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

Sécuriser les infrastructures

Du côté des fournisseurs de services numériques, les places de marché en ligne, les moteurs de recherche et les fournisseurs de services de Cloud actifs dans l'UE sont concernés. Ils devront prendre des mesures pour « assurer la sécurité de leur infrastructure » et signaler « les incidents majeurs » aux autorités nationales. Mais les exigences auxquelles devront se plier ces fournisseurs, seront moins élevées que celles applicables aux opérateurs de services essentiels.

Publication de la Directive NIS au Journal officiel de l'Union européenne
Adoption de la directive NIS : l'ANSSI, pilote de la transposition en France

---

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : Directive NIS adoptée: quelles conséquences pour les entreprises?

Cybersécurité et Cyberdéfense : leviers de l’intelligence économique

La transition numérique en Afrique étroitement liée à l’intelligence économique

---

La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. La cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les Etats.
Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson.
De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberespace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.
Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour l'attaquant…[lire la suite]

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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.

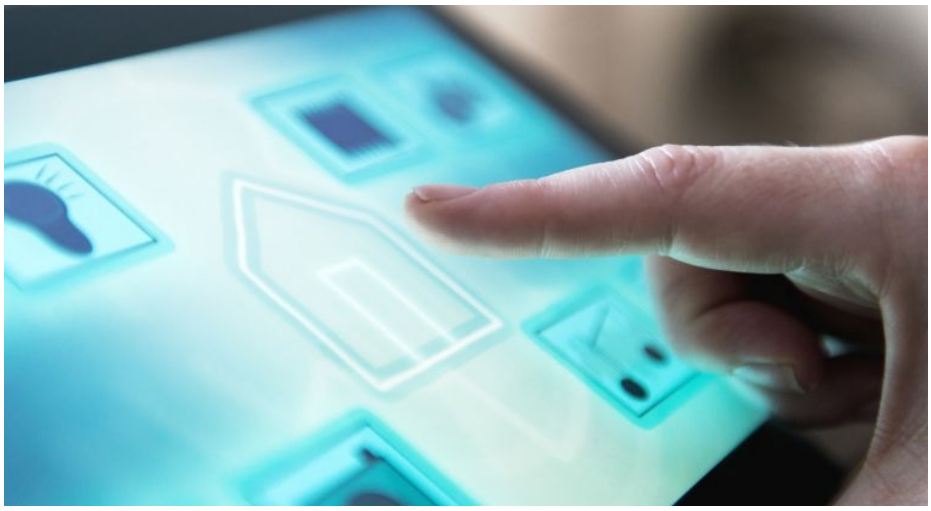
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité et Cyberdéfense : leviers de l’intelligence économique. »

Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?



Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

La Chine s'impose parmi les principaux pays créateurs d'objets quotidiens connectés à l'internet, mais elle génère ainsi de gigantesques failles sécuritaires exploitables par des pirates informatiques, a prévenu mardi John McAfee, créateur américain du logiciel antivirus portant son nom.

S'exprimant devant une conférence spécialisée à Pékin, M. McAfee a cité des précédents, dans lesquels des pirates sont parvenus à distance à prendre le contrôle de coffre-forts, de systèmes de chauffage, mais aussi d'ordinateurs de bord d'automobiles ou d'aéroplanes.

« La Chine prend la tête des progrès sur les objets intelligents, depuis les réfrigérateurs jusqu'aux thermostats, et c'est le maillon faible de la cybersécurité », a-t-il martelé, disant vouloir « lever un drapeau rouge » d'avertissement.
« Il y a tellement plus de ces objets, et plus vous en connectez ensemble, plus les risques de piratage augmentent », a encore souligné John McAfee.
L'excentrique septuagénaire avait fait fortune aux débuts d'internet dans les années 1990, après avoir mis au point un logiciel antivirus qui porte son nom et est maintenant la propriété d'Intel.
Plombé par la crise financière de 2008, il avait défrayé la chronique en 2012 après la mort de son voisin au Belize, pays où il vivait à l'époque et qu'il avait fui après l'ouverture d'une enquête de la police locale.
M. McAfee a livré à Pékin un discours au ton sombre et inquiétant, à l'heure où sa nouvelle société MGT Capital se prépare à lancer de nouveaux produits de cybersécurité d'ici la fin de l'année.
« Notre espèce n'a jamais été confrontée jusqu'ici à une menace de cette ampleur. Et pour l'essentiel, nous n'en prenons pas conscience », a-t-il averti.
« Vous pouvez penser que j'exagère, que je tombe dans l'alarmisme. Mais je compte parmi mes amis beaucoup de +hackers+ (pirates) qui ont les capacités de faire d'énormes dégâts si l'envie leur en prend », a-t-il ajouté.
A l'instar de Xiaomi, fabricant de smartphones ayant élargi son offre dans l'électroménager « intelligent », nombre d'entreprises chinoises intègrent désormais une connexion wi-fi à des produits variés, des autocuiseurs pour riz aux purificateurs d'air, permettant aux usagers de les allumer à distance depuis leur téléphone.
De telles connexions créent de graves failles qui accentuent les vulnérabilités de leurs réseaux, selon John McAfee.
Dans un entretien avec des journalistes à Pékin, l'Américain a cependant noté « n'avoir entendu parler d'aucune » attaque informatique de grande ampleur en Chine sur l'année passée, tandis que les Etats-Unis en enregistraient « des centaines ».

Original de l'article mis en page : Objets connectés : le créateur de l'antivirus McAfee met en garde la Chine contre les failles de sécurité | La Provence

---

Retrouver l'auteur d'un E-mail à partir de l'adresse IP

: Le demandeur condamné

Retrouver l'auteur d'un E-mail à partir de l'adresse IP : Le demandeur condamné

Le TGI de Meaux a débouté l'entreprise qui voulait obtenir de Numericable les noms, prénoms, adresses et coordonnées complètes de l'auteur d'un email frauduleux à partir de son adresse IP.

Dans une ordonnance de référé du 10 août 2016 repérée par Legalis, le tribunal de grande instance de Meaux (Seine-et-Marne) a débouté l'entreprise qui voulait obtenir de Numericable les données d'identification correspondant à l'adresse IP de l'auteur présumé d'un email frauduleux.
Comment en est-on arrivé là ? En début d'année, la société France Sécurité a préparé une proposition commerciale à l'attention d'Airbus Helicopters dans le cadre d'un appel d'offres. Dans la foulée, le distributeur d'équipements de protection individuelle a reçu un courriel d'un individu se faisant passer pour un employé d'Airbus et lui demandant de transmettre par courriel le fichier contenant la proposition… Suspectant la fraude, France Sécurité a contacté Airbus. Le nom associé au courriel était bien celui d'un de ses employés, mais il n'était pas l'auteur des courriels en question.

Usurpation d'identité
Dans un premier temps, une plainte a été déposée contre X pour usurpation d'identité. Parallèlement, le département informatique de France Sécurité a identifié l'adresse IP de l'expéditeur du courriel (transmis via Gmail) ainsi que le FAI hôte, à savoir : Numericable. Un procès-verbal de constat d'huissier a été établi. Ensuite, le 28 juin 2016, France Sécurité a déposé plainte auprès du procureur de la République près le tribunal de grande instance de Nantes. Et le 8 juillet 2016, l'entreprise a fait assigner devant le juge des référés du TGI de Meaux le câblo-opérateur. Le but : obtenir du tribunal qu'il ordonne au FAI de communiquer dans un délai de 48 heures les données d'identification correspondant à l'adresse IP en cause. Car, selon le demandeur, le câblo-opérateur est tenu de conserver les données permettant l'identification de son client et de déférer aux demandes de l'autorité judiciaire. Et ce en application de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004. France Sécurité souhaitait également qu'une astreinte soit versée par Numericable en cas de dépassement de ce délai, en plus des frais irrépétibles… Sans succès.

L'adresse IP, une donnée personnelle
Le juge est parti du principe que l'adresse IP est une donnée à caractère personnel. Par ailleurs, il a considéré que la collecte de cette donnée constitue un traitement au sens de la loi informatique et libertés. Une telle collecte aurait donc dû faire l'objet d'une autorisation de la Commission nationale informatique et libertés (Cnil) accordée à France Sécurité. Cela n'a pas été le cas. Par ailleurs, le juge considère que le cadre juridique applicable dans ce dossier ne peut pas être celui de la LCEN de 2004. Selon lui, Numericable n'est pas visé en tant que « personne dont l'activité est d'offrir un accès à des services de communication au public » en relation avec « la création d'un contenu » en ligne.
Résultat : le TGI de Meaux a débouté France Sécurité de toutes ses demandes. L'entreprise a été condamnée aux entiers dépens et au versement de 2 000 euros au titre des frais irrépétibles…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : IP : Numericable n’a pas à communiquer les données d’identification

---

Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

---

Cyber-risques liés à l'installation et l'usage de l'application Pokémon GoLancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.
Suite à la prise de conscience de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.
Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google.

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode « réalité augmentée » lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google. En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre « Sources inconnues » du menu « Sécurité »).
Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :
• d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
• de rechercher des comptes déjà présents sur l'appareil ;
• de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
• d'enregistrer localement des fichiers sur le téléphone.
Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.
Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.
Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9]…[lire la suite]

Original de l'article mis en page : Bulletin d'actualité CERTFR-2016-ACT-031