Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX

	Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX

Dans ses derniers correctifs pour MacOSX, Apple signale que plusieurs failles de corruption de mémoire ont été corrigées grâce à l'aide du CESG, l'équivalent britannique de l'Anssi rattaché au GCHQ.

Si les choses se passent plutôt mal entre le FBI et Apple, le constructeur semble entretenir des rapports bien plus cordiaux avec le GCHQ britannique. Celui-ci a en effet été crédité dans une note de patch pour avoir aisé à la correction de failles de sécurité au sein de MacOSX. Deux failles ont ainsi été corrigées à l'aide du CESG, l'une permettant une corruption de mémoire au niveau du kernel de Mac OSX et une autre au sein des technologies de gestion des ports Firewire. Celles-ci permettaient à un attaquant d'exécuter du code potentiellement malveillant sur la machine visée.

Ce n'est pas la première fois que le CESG est crédité pour avoir débusqué des failles au sein de logiciels et les avoir communiqué à l'éditeur. L'organisme est souvent présenté comme un équivalent britannique de l'Anssi, mais est de fait rattaché aux services du GCHQ, l'équivalent britannique de la NSA. Une position qui laisserait croire que celui-ci aurait plutôt tendance à garder les vulnérabilités découvertes par ses équipes pour ses activités d'espionnage informatique.

La collaboration entre les forces de l'ordre et les acteurs de l'IT est à géométrie variable. Si Apple semble travailler en bonne intelligence avec le CESG, ses rapports sont nettement moins apaisés avec le FBI. Aux États Unis, le FBI est d'ailleurs critiqué par les développeurs de Tor pour son refus de communiquer l'une des failles ayant été utilisées dans le démantèlement du réseau de pédopornographie Playpen. Le GCHQ tout comme le FBI ou la NSA ne donnent que peu d'information sur les raisons qui les poussent à dévoiler les failles qu'ils connaissent aux éditeurs des logiciels ou matériels affectés. Mais Apple ne crache pas dans la soupe et a profité du tuyau pour combler les deux failles signalées par le CESG… [Lire la suite]

Article de ZDNet

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

Source : *Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX – ZDNet*

Voici les 12 pays africains qui espionnent les comptes sur Facebook | CIO-MAG

Voici les 12 pays africains qui espionnent les comptes sur Facebook

Egypte, Algérie, Tunisie, Soudan, Sénégal, Côte d'Ivoire, Nigéria, Kenya, Ouganda, Tanzanie, Botswana, Afrique du Sud. Voilà les douze Etats africains qui surveillent les comptes des utilisateurs du réseau social Facebook. Selon Les Dépêches de Brazzaville, ces Etats sont cités par Facebook dans son dernier rapport de transparence. Y figurent au total 92 pays qui envoient, à travers le monde, des requêtes en vue d'obtenir des informations sur l'identité des utilisateurs de certains comptes Facebook ou de ses autres services de messagerie électronique. Il s'agit notamment de Messenger, Instagram et Whatsapp.

Accepter ou refuser ? Les conditions de Facebook

De ce rapport, il ressort que Facebook peut donner une suite favorable à une requête quand celle-ci porte sur une affaire criminelle. C'est le cas par exemple des requêtes du Nigéria dans le cadre des enquêtes sur les attaques terroristes du mouvement Boko Haram. Lorsqu'une requête est jugée recevable par Facebook, il permet au pays intéressé d'accéder aux données personnelles (noms, adresse, ancienneté, adresse IP) ou à la messagerie privée d'un utilisateur. Par contre, une requête est jugée non recevable lorsque Facebook ne perçoit pas le « bien-fondé légal » et le « factuel » de la demande. C'est ainsi que des requêtes du Sénégal et de l'Algérie ont été rejetées. Au 31 décembre 2015, plus de la moitié des requêtes reçues par le réseau social américain visaient à résoudre des affaires de vol ou d'enlèvement. A ce jour, Facebook totalise 126 785 000 utilisateurs en Afrique.

Article de Anselme Akéko

Réagissez à cet article

Source : *Voici les 12 pays africains qui espionnent les comptes sur Facebook | CIO-MAG*

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

---

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*

Un hôpital paye la rançon mais n’obtient rien en échange.

Un hôpital paye la rançon mais n’obtient rien en échange

Certains groupes de pirates qui exploitent des ransomwares pour faire fortune sans effort n'ont ni morale ni parole, si l'on en croit la prise en otage de données d'un hôpital, qui a payé pour rien la rançon demandée.

Les maître-chanteurs sont aussi parfois de véritables escrocs, et ça n'est jamais une bonne idée de céder à leurs exigences. Après la messagerie chiffrée Protonmail qui avait payé une rançon et avait malgré tout continué à subir des attaques DDOS massives, c'est un hôpital américain qui l'apprend à ses dépens.

Ainsi Network World rapporte que le Kansas Heart Hospital à Wichita a accepté de payer une rançon après que des pirates ont réussi à infecter son système informatique avec un ransomware, qui chiffre les données stockées avec une clé que seul le ravisseur connaît. Ce n'est pas le premier hôpital à être visé et à céder ainsi à un chantage informatisé, mais c'est la première fois que les pirates ne respectent pas leur part du marché. Pire, ils en demandent plus.

PAYER ENCORE POUR DÉBLOQUER UN PEU PLUS

L'attaque avait eu lieu la semaine dernière, et avait rendu des fichiers de l'hôpital inaccessibles, sans possibilité de recourir à des archives. Pour les débloquer, il fallait payer de l'argent en utilisant un service anonymisé, sur Tor, avec un compte en bitcoins intraçable. Étant donnée l'importance des données, les administrateurs de l'établissement ont accepté de payer une somme indéterminée, relativement faible. Mais plutôt que de déchiffrer les données, les pirates n'en ont libéré qu'une petite partie, et exigé davantage d'argent pour déchiffrer le reste.

L'hôpital a alors refusé. « Ce n'était plus une manœuvre sage ou une stratégie », s'est justifiée la direction, qui a mis en place un plan B pour limiter les effets de l'attaque. Selon le Kansas Heart Hospital, aucun patient n'a eu à subir d'effets négatifs en raison de l'indisponibilité de certaines données… [Lire la suite]

Réagissez à cet article

Source : *Ransomware : un hôpital paye la rançon mais n'obtient rien en échange – Business – Numerama*

Auteur : Guillaume Champeau

Furtim, le malware qui détruit les solutions de sécurité.

	Furtim, le malware qui détruit les solutions de sécurité

Alors que de nouveaux malwares sont découverts quasiment chaque jour, voilà que l'un d'entre eux fait beaucoup parler. Il s'agit de Furtim, un #logiciel malveillant qui se caractérise par sa faculté à détruire les solutions de sécurité présentes sur le PC infecté.

Si l'on en croit nos confrères de Silicon, un nouveau malware a été découvert par les équipes d'EnSilo. Comme son nom l'indique, Furtim est capable de passer inaperçu sur les machines qu'il a réussi à infecter.

Probablement crée par des hackers d'Europe de l'Est, ce malware se compose d'un driver qui scanne le PC infecté, d'un module downloader, d'un gestionnaire d'alimentation, d'un voleur de mots de passe et d'un module de communication serveur.

Toutefois, avec une telle composition, impossible de comprendre comment fonctionne réellement ce malware. Pour l'heure, Furtim apparait seulement comme un logiciel malveillant très sophistiqué et capable d'analyser son environnement avant de s'exécuter. Pour cela, il va scanner la machine infectée pour détecter les solutions de sécurité et les outils de filtrage DNS.

Preuve que les pirates ont pensé à tout, Furtim bloque l'accès à de nombreuses sites spécialisés dans la sécurité informatique et à des forums d'aide à la désinfection et désactive les notifications Windows, le gestionnaire des tâches et diverses autres fonctionnalités.

Furtim, un éclaireur en vue de futures attaques

Selon les premières recherches menées par les équipes d'EnSilo, Furtim n'aurait probablement pas vocation à agir seul puisqu'il pourrait bien uniquement jouer un rôle d'éclaireur.

En effet, puisqu'il est capable de déjouer les outils de sécurité, il pourrait être utilisé pour introduire des menaces sur des PC sans que cela ne soit décelable… [Lire la suite]

Réagissez à cet article

Source : *Furtim, le malware qui détruit les solutions de*

sécurité

Auteur : Fabrice Dupuis

---

11 millions volés dans une attaque simultanée de distributeurs automatiques

11 millions volés dans une attaque simultanée de distributeurs automatiques

---

Au Japon, des pirates ont réussi à dérober 1,4 milliard de yens (11 millions d'euros) à partir de 1.400 distributeurs automatiques à travers le pays en seulement deux heures. Cette affaire intrigue sérieusement la police japonaise. Des malfaiteurs sont parvenus à voler 1,4 milliard de yens (11 millions d'euros) à partir de 1.400 distributeurs automatiques de billets différents. L'affaire était dans le sac en moins de deux heures.

Cartes contrefaites

Ce vol a probablement été mené par un groupe international faisant usage de cartes de crédit contrefaites contenant des informations de compte dérobées à une banque sud-africaine. Le nom de la banque n'a pas été mentionné et Interpol compte bien aider la police nippone dans cette affaire, comme le rapporte The Japan Times. 14.000 transactions Plus de 100 personnes pourraient avoir coordonné ce retrait d'argent colossal. Le montant maximal de 100.000 yen a été retiré dans chacune des 14.000 transactions…. [Lire la suite]

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

M

Réagissez à cet article

Source : *(Mobile) – 11 millions volés dans une attaque simultanée de distributeurs automatiques*

Cybersécurité en Afrique : état des lieux et perspectives

Cybersécurité en Afrique : état des lieux et perspectives

Avec 20% de de sa population connectée à Internet, l'Afrique est un continent en voie de connexion au cyberespace. Une partie des pays du continent profite des retombées économiques du numérique mais ceux-ci doivent aussi faire face aux cybermenaces qui mettent en péril leur développement dans le cyberespace. Dès lors, comment se construit la cybersécurité en Afrique?

L'ENJEU DE LA CONNECTIVITÉ AVANT CELUI DE LA CYBERSÉCURITÉ

Avant d'évoquer pleinement la question de la cybersécurité en Afrique, il convient au préalable de poser une série de constats sur le niveau de connectivité du continent africain… [Lire la suite]

Article original : *Cybersécurité en Afrique : état des lieux et perspectives – SOLUCOMINSIGHT*
Auteur : JULIEN DOUILLARD Consultant

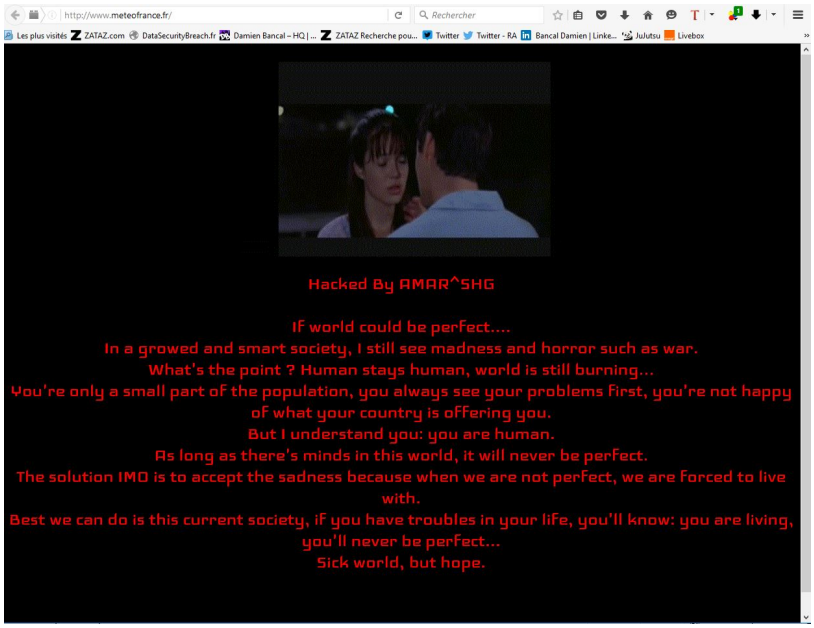
Réagissez à cet article

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

M

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.



Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

Détournement de DNS

Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « se plaignent pour leurs propres problèmes ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « Il faut vivre avec, avec espoir ».
Un message qui change des propos de haines, guerriers… que l'on peut croiser sur des pages modifiées par d'autres pirates informatiques. Une attaque qui a pu être mise en place via un phishing, un accès non autorisés à partir d'une injection SQL… Bref, plusieurs méthodes possibles ont pu être exploitées pour atteindre l'administration des noms de domaine et orchestrer ce détournement de DNS… [Lire la suite]

Réagissez à cet article

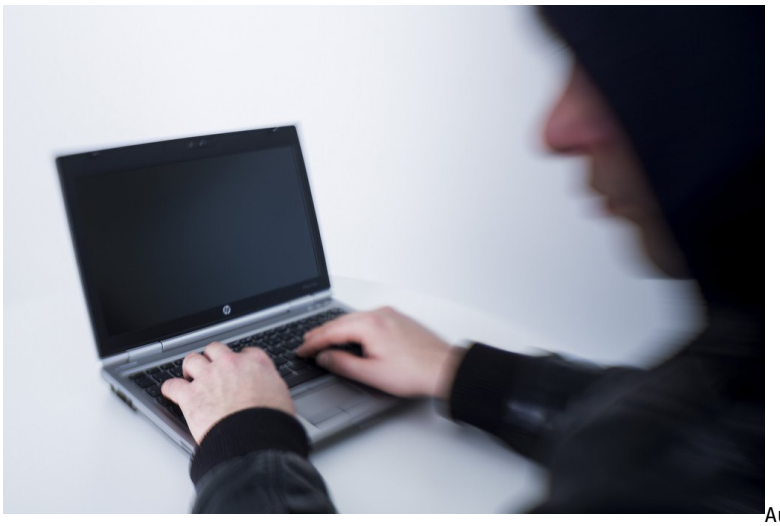
Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

La cybercriminalité fait des ravages dans les entreprises françaises.

La cybercriminalité fait des ravages dans les entreprises françaises

---

Selon une étude du cabinet PwC, le nombre d'entreprises françaises victimes de la cybercriminalité a presque doublé en deux ans.



Au cours des 2 dernières années, près de 70% des entreprises françaises ont été victimes de fraudes. On note notamment une forte hausse de la cybercriminalité, selon une étude effectuée par le cabinet Price Water House Coopers (PwC) publiée hier. La moyenne nationale est beaucoup plus élevée que celle mondiale.

La cybercriminalité visant les entreprises françaises explose

Les entreprises françaises sont-elles des cibles faciles pour les pirates ? Selon une étude de Price Water House Coopers concernant les fraudes en entreprises, les attaques informatiques occupent le deuxième rang derrière le détournement d'actifs. En 2 ans, la cybercriminalité a explosé en France, elle représente 53% des fraudes en 2016 contre 28% en 2014.

Aujourd'hui, une grande partie des entreprises (85%) ont pris conscience que le risque d'être victime de pirates informatiques est bel et bien réel. Elles n'étaient que 48% en 2014. Selon Louis Di Giovanni, travaillant dans le département Litiges et Investigations du cabinet PwC, « L'explosion du Big Data quels que soient les domaines, alliée à la digitalisation de l'activité économique et la multiplicité des supports numériques augmentent l'exposition des entreprises au risque de cyberattaque, d'où une plus grande prise en compte de ce risque par les dirigeants« .

Les entreprises françaises ne sont pas prêtes face à ce risque

Bien que les entreprises françaises aient bien pris en compte le risque élevé que représente la cybercriminalité, elles n'ont pas forcément mis en place de défenses adéquates. « Plus de la moitié des entreprises françaises n'ont pas encore de plan d'action 100% opérationnel pour répondre à une cyberattaque » déclarait M. Di Giovanni.

A cause de l'explosion de la cybercriminalité, le taux de fraude en entreprise progresse fortement. 68% des entreprises ont déclaré avoir été victimes d'une fraude au cours des deux dernières années, contre 55% en 2014, soit une hausse de 13 points… [Lire la suite]

L'étude PWC Global Economic Crime Survey 2016

Réagissez à cet article

Source : *La cybercriminalité fait des ravages dans les entreprises françaises*

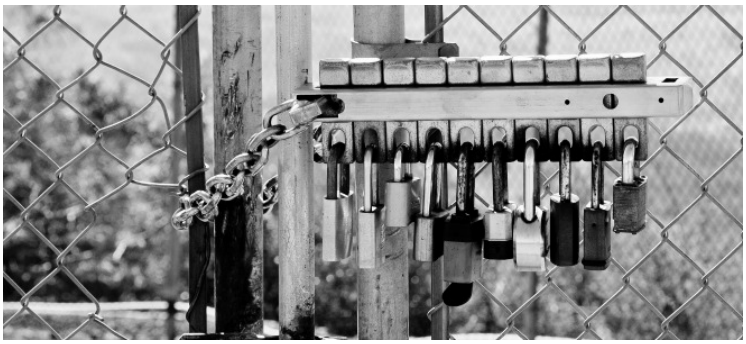
Auteur : David Pain

La sensibilisation des salariés à la Cybersécurité est essentielle

La sensibilisation des salariés à la Cybersécurité est essentielle

---

Bonne nouvelle : selon une étude menée par Solucom/Conscio Technologies et relayée par Les Échos, 82% des salariés sont sensibles aux risques informatiques et aux risques de vols d'informations. Mieux, 75% disent en avoir une bonne connaissance…. Des données intéressantes lorsque l'on sait que les failles de sécurité sont le plus souvent le fruit d'une négligence voire d'une malveillance humaine.



Une prise de conscience insuffisante ?

Si 88% des salariés disent être sensibilisés à l'enjeu de sécurité des mots de passe, dans les faits, ils ne sont que 47% à adopter les bonnes pratiques en la matière !

Parfois, les bonnes pratiques en elles-mêmes sont méconnues : 61% des salariés ne savent pas quoi faire à la réception d'un e-mail envoyé sous fausse identité, alors qu'ils sont 72% à se dire *sensibles* à la problématique.

On le voit, il y a un véritable enjeu pour les employeurs et les services IT : **mieux évangéliser, et ce de manière très concrète** pour que les salariés changent leurs comportements.

Quand implication et investissement vont de pair…

Un problème, donc, de communication en interne… Et, aussi, de moyens ? D'après une autre étude mentionnée par Les Échos, deux-tiers des responsables de service informatique considèrent que les budgets alloués par leur entreprise à la cybersécurité sont insuffisants.

=> L'étude, vue par Les Échos

Une formation infdispensable

Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises | Denis JACOPINI

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

Source : *Cybersécurité : appuyez-vous sur vos salariés ! | Microsoft pour les PME*