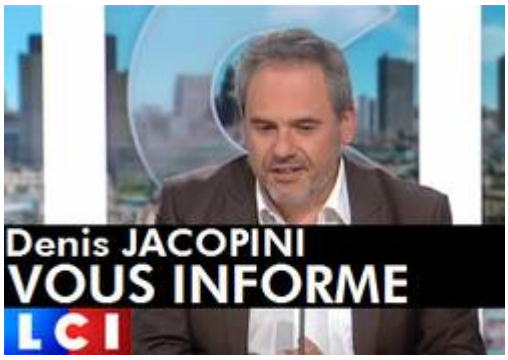
Les autorités s’inquiètent des piratages visant les avions



Les autorités s’inquiètent des piratages visant les avions

L’agence européenne chargée de la sécurité à bord des avions s’inquiète des possibilités de pirater les systèmes informatiques embarqués.

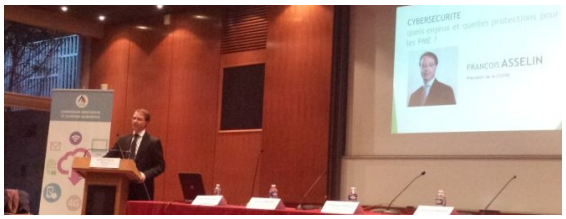
L’autorité a fait appel à un hacker, qui est parvenu à pénétrer plusieurs systèmes de communication.
L’Agence européenne de sécurité aérienne (AESA) insiste sur le manque de sécurité sur certains équipements embarqués dans les avions. Selon son directeur, Patrick Ky, des hackers pourraient facilement prendre le contrôle de plusieurs systèmes, en particulier lorsque les engins se trouvent encore au sol.
Le responsable appuie ses craintes par une expérience menée avec un hacker. Ce dernier serait parvenu à pénétrer en quelques minutes un réseau baptisé Acars (Aircraft Communication Addressing and Reporting System). Ce dernier sert aux compagnies aériennes à s’envoyer des messages automatiques entre les avions et le sol. Ces données communiquent des informations sur l’état de l’avion et ses éventuelles avaries sur ses installations critiques.
Le risque en termes de sécurité est avéré, selon les dires du responsable. Il convient toutefois de préciser que le système en cause n’est pas connecté avec les dispositifs contrôlant les avions. Il n’est donc pas question de prendre la main à distance sur un engin volant.Su
ite à ces révélations, l’AESA s’inquiète de la multiplication des systèmes de communication entre les avions mais également les satellites ou les installations présentes au sol. Cet accroissement pourrait tout aussi ajouter de nouveaux risques de piratages. C’est pourquoi l’organisme milite pour que les autorités américaines et européennes se rapprochent autour d’un projet commun d’analyse de données du trafic aérien.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-782578-piratage-avion.html

Le président de la CGPME avoue aussi avoir été victime de piratage informatique

	Le président de la CGPME avoue aussi avoir été victime de piratage informatique

Sous l'impulsion de son nouveau président François Asselin, la CGPME compte mettre l'accent sur le numérique. Elle a organisé mercredi 18 novembre sur Paris une session spéciale TPE-PME et cyber-sécurité.



On ne va pas se voiler la face : il y a du boulot sur la sensibilisation au thème de transition numérique pour les TPE-PME.
Un segment vraiment délaissé par les éditeurs alors qu'il correspond à une vraie représentation du tissu économique en France.
Sur les 3 millions d'entreprises en France, une proportion d'1,6 million d'entre elles dispose d'un effectif situé dans une fourchette 1 – 250 salariés.
Et les entreprises concernées se sentent bien seules car l'offre de produits et services n'est pas adaptée à leur besoin.
Alors qu'elles ont besoin de conseils personnalisés dans le domaine du numérique afin que les dirigeants d'entreprises puissent se concentrer sur leur cœur de métier.
[…]
Le témoignage le plus poignant et le plus concret rencontré sur le terrain, c'est François Asselin qui l'a délivré en clôture. Il reflète bien les problématiques auxquelles les PME sont confrontées.
En prenant la parole, François Asselin relate sa mésaventure qui a failli aboutir à la perte de son entreprise familiale de charpente, menuiserie, ébénisterie et ferronnerie d'art (147 salariés avec des serveurs sur trois sites), installée dans les Deux-Sèvres.
« Le problème de la cyber-sécurité, je l'ai vécu il y a plus d'un an et demi », lance François Asselin.
Tout part de l'ouverture d'un mail avec une pièce jointe, qui semblait reprendre un fichier d'entreprise. Mauvaise pioche : c'est un malware, qui rend tous les fichiers de l'entreprise inaccessibles (un volume de 420 000 documents) et fait tomber tous les serveurs.
Le piège du rançongiciel (ramsonware) est tendu. « Un message classique m'attendait sur le site Internet : il fallait que je verse X milliers d'euros en équivalent bitcoins pour récupérer la clé de déverrouillage de mes fichiers. »

Qui contacter en cas de pépin ?

L'anecdote du commissariat de Thouars (siège social de l'entreprise) est croustillante. François Asselin se souvient encore de la scène alors qu'il vient expliquer la situation avec le problème de son ordinateur avec copie d'écran.
« Je me souviens de l'accueil de la fonctionnaire : Hey chef, venez voir !
– Ah bah ça alors ! s'exclame le chef.
– Oui je viens porter plainte, poursuit François Asselin.
– C'est compliqué : comment on qualifie la plainte », s'interroge le supérieur.

Après ce vaudeville numérique, le niveau de la discussion remonte avec la préfecture des Deux-Sèvres contactée. *« Un interlocuteur était parfaitement au courant déjà à l'époque sur ce genre de mésaventure. »*
La situation aurait pu se transformer en catastrophe : *« Nous n'avions plus aucun accès aux logiciels : devis des clients, paie des salariés, facturation des fournisseurs…Cela aurait pu devenir une vraie catastrophe si nous n'avions pas sauvegardé les informations. Ca a sauvé la boîte, sincèrement. »*
Car la société Asselin SAS avait pris le soin de recourir depuis quelques années à une petite société de services informatiques pour assurer l'infogérance de l'entreprise.
« La réponse à ce souci de cyber-sécurité, c'est la qualité de la sauvegarde. Il a fallu 34 heures pour ré-installer les fichiers en place. On a perdu presqu'une journée de travail mais ce n'est pas dramatique. »

Cyber-sécurité : il faut en parler

Fort de cette expérience marquante, François Asselin a pris ce sujet à bras le corps et compte s'appuyer sur la commission Innovation et Economie numérique de la CGPME pour adresser la bonne parole.
« Cette aventure malheureusement, nous sommes assez nombreux à la connaître. Mais très peu d'entreprises ont porté plainte. Parce que l'outil numérique n'est pas devenu aussi indispensable que cela pour certaines entreprises. Ce n'est pas forcément une catastrophe en cas de perte. »
Mais la situation risque d'être critique en pleine transition numérique des entreprises.
Trop alarmiste ? Le président de la CGPME reprend l'exemple de l'entreprise BRM Mobilier de Bressuire (également situé dans les Deux-sèvres). Celle-ci est menacée de fermeture en raison d'une escroquerie de type « fraude au président » qui a siphonné dans le courant de l'été sa trésorerie d'un montant de 1,6 million d'euros.
Une enquête a été ouverte pour escroquerie en bande organisée.

François Asselin demande aux sociétés membres de la confédération qu'il dirige de « prendre des mesures de bon sens ».
« Sur le volet de la dématérialisation, assurez-vous de la qualité de transmissions des fichiers. Ne vous ruez pas sur le premier opérateur ou service gratuit, formez-vous à l'archivage numérique. On le fait correctement pour la version papier mais on est plus léger dans la version numérique. »
Le message est plus global : « On entend souvent parler des attaques visant des grands groupes mais il y a des PME qui sont victimes. On en mesure mal le nombre. Malheureusement, les PME sont trop silencieuses, nous avons un devoir d'évoquer ce sujet. »
En revenant sur son cas individuel, François Asselin rencontre un écueil en termes d'interlocuteurs adéquats : comment se faire accompagner par des professionnels dans le numérique qui répondent aux vrais besoins des TPE/PME. Le tout avec un budget raisonnable.
« Faire appel à une grande société informatique pour me mettre des firewall en cascade, c'est dépenser beaucoup d'argent en n'étant jamais efficace. La meilleure des efficacités, ce sont des choses de bon sens. Révisez vos procédures dans l'entreprise. C'est le meilleur moyen pour éviter la fraude au président qui fait des ravages. »

Cyber-attaques, vigilance rouge pour les maires et les administrations

Cyber-attaques, vigilance rouge pour les maires et les administrations

Les cyber-attaques sont aussi une arme utilisée par les terroristes. Les maires et les administrations les craignent à juste titre. Conseils de l'ANSSI.

Dans un entretien publié dans le journal Le Monde du 10 novembre, le directeur de l'ANSSI (Agence nationale de sécurité des systèmes d'information) alerte sur une autre facette du terrorisme, les cyber-attaques.
Cela inquiète d'ailleurs de nombreux maires ruraux et les administrations qui ont encore en mémoire la cyber-attaque contre TV5 Monde, ce début d'année et les nombreux « défaçage » de sites administratifs. Celui-ci consiste à remplacer leurs pages d'accueil par des slogans faisant l'apologie du terrorisme ou en les sabotant.

D'où les conseils suivants de l'ANSSI :
1.- contacter le prestataire informatique qui a réalisé le site web ou l'hébergeur du site,
2.- vérifiez avec eux que toutes les mises à jour ont bien été réalisées surtout celles des pare-feux,
3.- créer des copies de sauvegarde des fichiers corrompus afin de les remettre aux enquêteurs,
4.- porter plainte auprès de la police ou de la gendarmerie puisque ces actes peuvent tomber sous le coup de la circulaire 2015/0213/A13 du 12 janvier 2015 du ministère de la justice (voir lien ci-dessous)

Pour se prémunir et éviter que cela se produise, l'ANSSI conseille :
1.- utiliser des mots de passe robustes d'au moins 12 caractères alternant majuscules, minuscules, chiffres et symboles,
2.- éviter un même mot de passe pour des accès différents,
3.- ne pas configurer les logiciels pour qu'ils retiennent les mots de passe,
4.- faire les mises à jour depuis le poste informatique, en aucun cas à distance depuis un ordinateur extérieur, une tablette ou un Smartphone,
5.- mettre à jour tous les logiciels afin de corriger les failles,
6.- réaliser une surveillance du compte ou des publications en prévoyant des sauvegardes. Attention aux courriels et leurs pièces jointes- toujours vérifier la cohérence entre l'expéditeur et le contenu du message,- ne pas ouvrir les pièces jointes provenant de destinataires inconnus ou douteux,- passer la souris sur les liens avant de cliquer afin que l'adresse complète s'affiche,- ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles.

Bien évidemment, ces mesures ne font pas écran total contre les cyber-attaque mais permettent quand même un minimum de prévention.
Elles permettent aussi aux maires (responsables de l'état-civil par exemple) et aux administrations qui détiennent de nombreux fichiers de clients et les comptes bancaires de se « couvrir » pour garantir la sécurité des données à caractère personnel que contiennent leurs sites Internet.

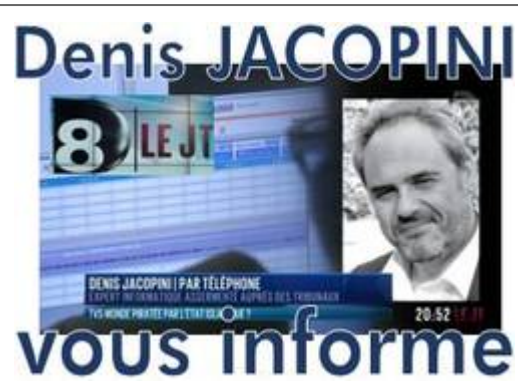
Liens :
– site de l'ANSSI :
http://www.ssi.gouv.fr

– circulaire du ministère de la justice :
http://www.justice.gouv.fr/publication/circ_20150113_infractions_commises_suite_attentats201510002055.pdf
– signaler : www.internet-signalement.gouv.frwww.signal-spam.fr

---

Source : http://www.humanite.fr/cyber-attaques-vigilance-rouge-pour-les-maires-et-les-administrations-589915

Face à la hausse des cyberattaques en Tunisie, ESET lance ses nouvelles solutions



Face à la hausse des cyberattaques en Tunisie, ESET lance ses nouvelles solutions