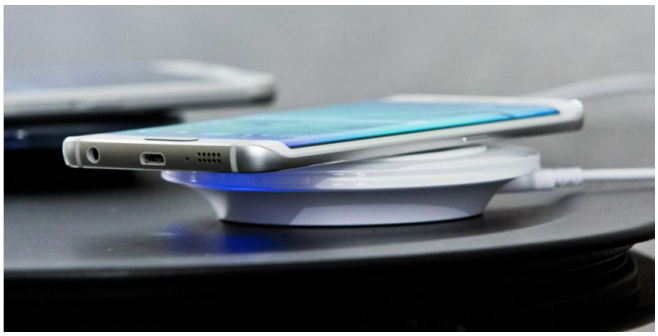
Samsung Galaxy S6 et S6 Edge : sans le savoir, vous êtes (peut-être) sur écoute

Samsung Galaxy S6 et S6 Edge : sans le savoir, vous êtes (peut-être) sur écoute

Voilà une information qui ne devrait pas ravir les utilisateurs de smartphones de la marque Samsung. Une équipe de chercheurs en sécurité informatique vient d'annoncer avoir découvert une faille permettant d'écouter les conversations téléphoniques émises depuis les Galaxy S6 et S6 Edge.



En vrai, c'est plutôt une bonne nouvelle ! Explications.
Rassurez-vous, les ingénieurs de Samsung sont déjà sur le coup pour corriger la faille de sécurité;
On a du mal à y croire, et pourtant une équipe de chercheurs en sécurité informatique a découvert l'existence d'une faille permettant d'écouter les conversations téléphoniques des possesseurs de smartphones de la marque Samsung.
Le problème a été révélé par deux experts Daniel Komaromy et Nico Goldelors lors du Mobile Pwn20wn de PacSec à Tokyo, un concours de hackeurs « gentils » pour tester la sécurité des produits high-tech.
Il s'agit d'une attaque de type « Man in the Middle ». En langage informatique, l'attaque dites de « l'homme du milieu » est une technique qui consiste pour un hackeur à s'interposer entre vous et votre destinataire dans le but d'intercepter les échanges qui ont lieu.
Pour ce faire, toutefois, cela nécessite d'installer une station d'écoute à proximité du smartphone espionné. Ce qui est loin d'être à la portée de tous, évidemment.

Capter les conversations, sans que l'utilisateur ne le sache

Tous les téléphones mobiles, et plus généralement tous les appareils de communication mobile, fonctionnent en réalité avec deux systèmes d'exploitation qui tournent l'un à côté de l'autre. Le premier, tout le monde le connaît : il se nomme Android, iOS, Windows Phone ou BlackBerry. L'autre est moins connu : il se trouve sur une puce électronique située dans la base du téléphone, qui permet de gérer les appels vocaux émis depuis le smartphone (appelé baseband).
Lorsque le téléphone est connecté à un réseau (mobile ou internet), la station d'écoute installée préalablement envoie un petit logiciel (un firmware, en langage informatique) qui permet de pirater cette puce électronique. Les communications peuvent alors être captées par un hackeur, à distance, sans que l'utilisateur ne puisse s'en apercevoir.

Une autre faille découverte sur l'appli Chrome Android

Rassurez-vous, les ingénieurs de Samsung sont déjà sur le coup pour corriger la faille ! Les deux chercheurs en sécurité informatique n'ont pas dévoilé publiquement l'ensemble de la procédure, pour éviter toute tentation. Un rapport détaillé a été remis à Samsung.
À l'instar de Google, le géant coréen propose désormais des mises à jour de sécurité mensuelles : la prochaine est disponible dans les prochains jours.
Lors du même événement, une autre faille a été décelée concernant cette fois le navigateur Chrome sous Android. Grâce à cette faille, il serait possible d'installer une application sur n'importe quel appareil Android, et sans que l'utilisateur ne puisse s'en apercevoir.

Source :
http://www.metronews.fr/high-tech/samsung-galaxy-s6-et-s6edge-sans-le-savoir-vous-etes-peut-etre-sur-ecoute/moks!xGbp39O9FvRQ/

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. »

Régionales 2015 : la CNIL précise l’encadrement des fichiers de communication politique

A l'approche des Régionales 2015, la CNIL a relancé son dispositif d'alerte à destination des électeurs qui viendraient à se plaindre d'une pluie de courriers non sollicités.

Elle distille par la même occasion plusieurs informations au profit des candidats et des partis politiques afin d'encadrer leur propagande politique.

La Commission Informatique et Libertés vient de mettre en ligne un outil destiné à glaner le témoignage des électeurs qui se plaindraient d'un spam politique, ou de toute autre bisbille avec un candidat aux élections régionales.

Cette initiative est une branche de l'observatoire destiné à accompagner les partis et les candidats dans leurs futures opérations de communication politiques.

Sur ces pages, elle rappelle par exemple que les électeurs ont la possibilité de s'opposer « à la collecte d'informations les concernant, notamment leur identité et leurs coordonnées », ainsi, « les personnes prospectées (appel à dons, à rejoindre un parti politique ou la structure soutenant un candidat…) peuvent s'opposer sans avoir à justifier de motifs légitimes. »

Fichiers prospects ou listes électorales

De même la Commission revient sur les différentes hypothèses qui permettent à un candidat ou un parti politique d'arroser les boites aux lettres de propagande électorale.

Outre le consentement spécifique de la personne, un candidat peut acheter ou louer un fichier de clients ou de prospects à des fins de propagande politique. Sauf que plusieurs règles de base encadrent cette exploitation : seuls ces fichiers peuvent servir de tremplin, donc « pas le fichier de gestion de la paye des salariés, par exemple ».

Autre chose, cette potentielle exploitation doit avoir été prévue dans la déclaration auprès de la CNIL, soit dès le départ soit après une modification.

De même, la CNIL prévient qu'il « n'est pas possible de sélectionner les destinataires du message de communication politique sur la base de la consonance de leur nom ou sur leur lieu de naissance ». Surtout, en amont, les personnes ciblées devront être informées « de la possible utilisation de leurs données à des fins de communication politique. »

Droit d'opposition

Sur le droit d'opposition, celui-ci varie en fonction de la source. Les personnes peuvent par exemple s'opposer à la réception de nouveaux mails fruits de ces fichiers. Par contre, il n'est pas possible de s'opposer à recevoir la propagande électorale officielle adressée aux personnes inscrite sur la liste électorale, qui est un autre puits à communication politique.

Dans cette dernière hypothèse, les droits sont plus restreints côté électeurs. « Vous ne pouvez pas refuser que les informations vous concernant figurant sur la liste électorale soient utilisées à des fins de propagande politique par les candidats ou les partis » indique par exemple la CNIL. Cependant, « vous pouvez demander à un candidat ou un parti de ne plus vous envoyer de messages. »

Dans le passé la CNIL avait déjà sanctionné une commune pour avoir diffusé des éléments de la liste électorale sur Internet au-delà des dates prévues par le Code électoral. Pour cette année, la même commission a mis en ligne un guide pratique complet sur les obligations légales et les bonnes pratiques à suivre : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Politique.pdf

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Source : http://www.nextinpact.com/news/97318-regionales-2015-cnil-precise-encadrement-fichiers-communication-politique.htm

Plus de 8 Français sur 10 sont inquiets concernant la protection de leurs données personnelles sur Internet

Plus de 8 Français sur 10 sont inquiets concernant la protection de leurs données personnelles sur Internet