Quels sont les risque des photos de vos jeunes enfants sur Facebook ?

Quels sont les risque des photos de vos jeunes enfants sur Facebook ?

Une vigilance s'impose et la question à se poser est de savoir comment une photo postée à un instant donné pourrait être perçu X années plus tard sachant que nous ne maîtrisons pas tout quant aux futurs possibles.

Et qui peut la consulter directement ou non. Il convient de savoir si ses amis sont sûrs et de s'assurer de l'identité véridique d'une personne demandant à rentrer en contact avec soi pour éviter les usurpations d'identité potentielles. Facebook et les autres outils – même Snapchat où les courtes vidéos peuvent être récupérées – n'ont rien de journaux intimes.
Par ailleurs, il est possible de réserver des comptes pour ses enfants sans les utiliser pour éviter tout conflit avec des homonymes éventuels – certes, Facebook demande que l'on soit majeur numériquement, c'est-à-dire âgé d'au moins 13 ans, mais c'est peu vérifié dans les faits. Mais plus que tout, il convient d'éduquer ses enfants quant au monde numérique et ses pièges en l'étant au préalable soi-même. Un dialogue peut être noué entre enfants et parents mais dans le cadre d'un bébé ou d'un enfant de quelques années, c'est le parent qui est responsable des traces qu'il va léguer à son enfant, d'où une vigilance supplémentaire pour ne pas d'emblée lui entacher sa réputation numérique : photos de l'enfant nu, grimaces, etc. L'utilisation des tags est à manier avec précaution et mieux vaut ne pas reconnaître une personne sur une photo, ce qui fait avant tout le jeu de Facebook ou d'autres outils mais qui n'est pas l'intérêt premier de la personne.
Article de David Fayon. Propos recueillis par Thomas Gorriz

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 : Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook | Atlantico.fr

---

Facebook regarde dans quels magasins vous faites vos courses

Facebook regarde dans quels magasins vous faites vos courses

Facebook va désormais traquer les données de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but est de permettre aux annonceurs de savoir si leurs publicités attirent des consommateurs sur leurs points de vente.

Facebook ne cesse de renforcer son service de publicités. Le réseau social veut proposer une offre plus précise et pertinente pour ses clients. Pour cela, il se servira désormais des données de localisation de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but ? Permettre aux entreprises de savoir si leurs annonces sur Facebook attirent du monde dans leurs magasins.

Ainsi, les annonceurs pourront comparer le nombre de personnes qui ont vu leurs annonces au taux de fréquentations de leurs points de vente. Ils peuvent également intégrer une carte interactive à leur publicité – sous la forme d'un carrousel – pour indiquer à l'internaute le chemin qui le mènera au magasin le plus proche.

Ces nouvelles fonctionnalités s'inscrivent dans une volonté de Facebook de proposer des services plus personnalisés – et donc plus efficaces – à ses clients. En 2014, la boîte de Mark Zuckerberg avait déjà lancé une plateforme qui permet d'afficher de la publicité aux utilisateurs du réseau social qui se trouvent à proximité du magasin afin de les inciter à s'y rendre rapidement.

Selon Facebook, plusieurs entreprises ont déjà eu l'occasion de tester, en avant-première, ces nouvelles fonctionnalités. Parmi eux, se trouve E.Leclerc. La chaîne de distribution française « a pu atteindre 1,5 millions de personnes dans un rayon de dix kilomètres autour de ses supermarché et a observé qu'environ 12 % des clics sur leur publicité ont entraîné une visite en magasin dans les sept jours qui suivaient », indique Facebook dans son annonce.

Grâce à ces jeux de données très précis, Facebook fournit des outils pertinents pour les entreprises car, grâce à cela, elles peuvent ajuster leur stratégie de communication en fonction de chaque point de vente et de chaque région. Le réseau social prouve encore plus à quel point il représente un atout bien plus puissant que les modes de diffusion traditionnels.

Quant aux utilisateurs de Facebook, si cette information a de quoi énerver, elle n'a rien de vraiment surprenant. Il est de notoriété publique que la publicité ciblée représente le fonds de commerce principal du réseau social. Celui-ci n'est d'ailleurs pas le seul à traquer les internautes pour savoir dans quels magasins ils vont. Google le fait depuis quelques temps déjà, comme le rappelle, dans un tweet, Jason Spero, responsable de la stratégie et des ventes mobiles chez la firme de Moutain View.

Google dispose de données encore plus importantes destinées aux annonceurs et adapte les publicités en fonction, entre autres, des recherches de l'utilisateur et de sa géolocalisation.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Facebook regarde dans quels magasins vous faites vos courses – Business – Numerama

---

La double authentification de

Google contournée par des hackers

La double authentification de Google contournée par des hackers

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient.

Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

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

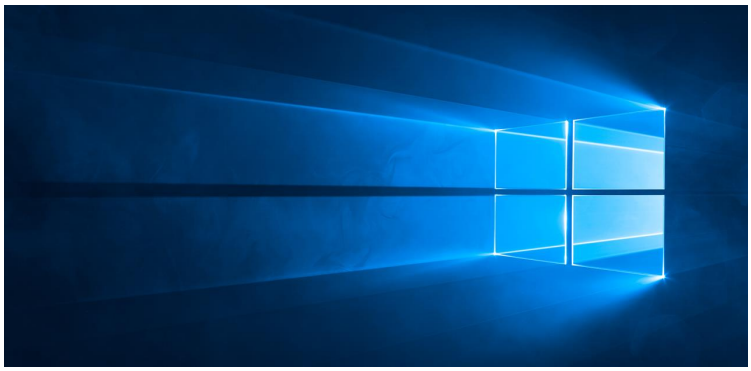
Original de l’article mis en page : La double authentification de Google contournée par des hackers

---

Microsoft corrige 44 failles de sécurité

	Microsoft corrige 44 failles de sécurité

Microsoft vient de publier une nouvelle mise à jour cumulative pour Windows 10. Elle reprend tous les correctifs de sécurité sortis depuis la dernière, mais ajoute comme d'habitude une série d'optimisations.



Patch Tuesday oblige, toute une série de bulletins de sécurité a été émise par Microsoft. 16 sont disponibles, dont 5 critiques (DNS, Office, JScript/VBScript, Edge et Internet Explorer), pour un total de 44 vulnérabilités colmatées. Toutes les versions de Windows et Office en cours de support sont touchées et il faut donc procéder à la récupération des mises à jour depuis Windows Update.

Correctifs de sécurité et réparations diverses

Dans le cas de Windows 10, cela donne lieu à une nouvelle mise à jour cumulative. Tous les correctifs de sécurité nécessaires y sont bien sûr, mais d'autres réparations sont disponibles, Microsoft restant sur son rythme d'amélioration continue de sa plateforme.

Les apports proposés sont nombreux et concernent aussi bien une meilleure fiabilité pour des composants comme Edge, Cortana, la lecture de sons, Cartes, Miracast et Explorer, que des corrections de bugs divers. Ces derniers concernaient par exemple l'affichage des bulles de notifications qui apparaissaient parfois en haut à gauche de l'écran, des solutions VPN qui ne fonctionnaient plus après certaines bascules entre cartes réseau, une position géographique qui n'était pas aussi rapidement mise à jour que nécessaire, et ainsi de suite.

Les smartphones aussi sont mis à jour

Notez que Windows 10 oblige, cette nouvelle version du système, estampillée 10586.420, se répercute également sur la mouture Mobile. Tous les smartphones l'utilisant peuvent donc se rendre dans la zone des mises à jour pour la récupérer. Il n'y a pas de liste spécifique des nouveautés, mais puisque la plupart des composants et des applications sont les mêmes que pour la mouture PC, les améliorations le sont également. On trouve mention toutefois d'un problème réglé pour lessmartphones : la sonnerie du téléphone qui s'interrompait parfois à la réception d'un SMS.

On rappellera que ces mises à jour cumulatives s'adressent pour l'instant toujours à la version 10586 mise en place initialement avec l'évolution majeure de novembre dernier, surnommée TH2, pour « Threshold 2 ». À la fin du mois prochain arrivera RS1, pour « Redstone 1 », sous la forme d'une Anniversary Update. Elle sera considérée comme le nouveau socle, déclenchant à son tour une nouvelle série de mises à jour cumulatives mensuelles.

Pour l'heure, tous les appareils disposant au minimum de Vista devraient être mis à jour sans attendre.

Article original de Vincent Hermann

Réagissez à cet article

Original de l'article mis en page : Microsoft : 44 failles colmatées et mise à jour cumulative pour Windows 10 — Next INpact

Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook

Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook

Atlantico : Poster une photo de son enfant sur Facebook peut-il lui porter préjudice ? Si oui, quand ? Et pourquoi ?

Publier une photo de ses enfants sur Facebook – qui est de loin le leader des réseaux sociaux dans le monde – est un acte compréhensible mais qui fait surtout plaisir sur le moment aux parents. Les parents façonnent l'identité numérique de leurs enfants à l'insu de leur plein gré alors même que le droit à l'oubli n'existe pas sur Internet. Plus tard, certaines traces numériques (photos ou vidéos postées avec les commentaires et tags associés) peuvent être utilisées contre eux surtout si les paramétrages de confidentialités sont mal utilisés.

Et même en postant une photo accessible aux seuls amis, celle-ci peut ensuite être partagée plus largement. En outre les personnes qui vont réagir à la photo permettent de révéler l'écosystème relationnel de la personne. Il est facile d'établir des corrélations entre les personnes. Et en fonction du profil des personnes réagissant de déterminer quel est le profil potentiel de l'enfant sur la photo. Pour les préjudices, on pense avant tout à l'attitude d'un recruteur mais ce peut être aussi des amis potentiels de l'enfant qui le jugeront avec un autre regard. Déjà on google une personne avant de la rencontrer ce qui induit un prisme dans la première rencontre. Le préjudice peut intervenir à des périodes charnières de la vie : adolescence où l'individu se construit et est sensible au regard des autres, entrée dans la vie active, rencontre amoureuse, etc.

Comment fonctionne le système de tag ? Quelle est sa fonction ? Pourquoi l'utilise-t-on ?

Il s'agit d'un système mis en place par Facebook qui permet à un utilisateur de Facebook d'indiquer qu'une personne figure sur une photo. En quelque sorte, un traitement manuel du facebooknaute lui-même vient en complément de l'algorithme mis en place par Facebook pour collecter des données personnelles (en l'occurrence les photos des visages des personnes) de nature à faire grandir la base d'information relative à une personne. Facebook peut avec l'expérience lui-même déterminer les personnes reconnues sur les photos, ce qui est parfois bluffant. Facebook peut ensuite, en fonction des références à d'autres posts, déterminer le cercle probable de personnes autour de celle qui a été taguée. Ceci lui permet de faire des suggestions (par exemple amis que l'on pourrait connaître, voire produits ou services que l'on est susceptible d'aimer car les goûts de ses amis sont souvent plus proches des siens que ceux d'inconnus) avec des taux de retour plus pertinents.

L'objectif de Facebook est d'exploiter le *big data* constitué par les photos et leurs tags pour sans cesse améliorer les résultats pour les marques partenaires et qui paient ses services. Par ailleurs, les algorithmes qui permettent de reconnaître les visages et les techniques de bio-identification ne sont qu'à leur début. Demain, à partir d'une simple photo, il sera, avec des outils idoines, possible de dresser le portrait robot d'une personne en allant fouiller sur l'ensemble de la webosphère (pas seulement sur Facebook mais sur l'ensemble des réseaux sociaux et des sites) pour collecter les numéros de téléphone, les adresses mails et d'autres détails personnels associés. Ceci peut présenter des opportunités réelles pour mieux connaître rapidement une personne, mais présente des risques. Des garde-fous et une éthique sont à construire pour éviter que le numérique ne soit un facteur d'exclusion ou un moyen d'ostraciser les internautes. Alors que les États-Unis sont dans le mécanisme d'*opt-out* (utilisation *a priori* des données personnelles sans autorisation préalable), l'Europe préfère l'*opt-in* qui constitue un principe de précaution quant à l'exploitation des données personnelles. Mais force est de constater que les outils majoritairement utilisés en Europe sont Américains et que nous sommes GAFA-dépendant *(Ndlr : GAFA = Google, Apple, Facebook, Amazon)* et qu'en contrepartie de la gratuité d'utilisation d'un service, nous fournissons et souvent avec beaucoup de zèle des données personnelles que ces outils utilisent à la fois avec un traitement automatique et un traitement humain qui le perfectionne comme celui des tags.

Article original de David Fayon Lire la suite…

Réagissez à cet article

Original de l’article mis en page : Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook | Atlantico.fr

---

Trois étapes pour mieux protéger les données en mobilité

Trois étapes pour mieux protéger les données en mobilité

Pour mieux protéger les données en mobilités, la DSI doit connaître les spécificités de chaque système d'exploitation mobile, déterminer quels terminaux accepter dans l'environnement de travail, et comprendre les capacités natives de protection des données.

Protéger les données d'entreprise contre la perte et le vol est l'une des principales priorités. Les brèches de données sont douloureuses et onéreuses. Et leurs effets peuvent être étendus, entre atteinte à la marque et sanctions réglementaires.
Heureusement, l'industrie du mobile a progressé dans la prise en compte des préoccupations des entreprises en matière de sécurité, tout particulièrement pour ce qui est de la protection des données en mobilité. Par le passé, les smartphones manquaient de capacités même basiques de chiffrement des données. Mais ils ont depuis évolué en plateformes dotées de capacités de sandboxing avancées.
Parallèlement, les suites de gestion de la mobilité d'entreprise (EMM) ont amélioré le contrôle et la surveillance via le réseau, en OTA (over-the-air), ce qui donne aux DSI une pléthore d'outils de protections des données en mobilité, qu'elles transitent sur le réseau de l'entreprise ou via un point d'accès à Internet public.

Tout part du système d'exploitation mobile
La plupart des postes de travail des entreprises fonctionnent sous Windows, voire sous OS X. Cela offre aux DSI un environnement relativement cohérent et maîtrisé. Mais les terminaux mobiles exécutent des systèmes d'exploitation plus variés et évoluant plus rapidement, susceptibles d'ailleurs de changer d'un constructeur à l'autre, sinon d'un modèle à l'autre. Lorsque les utilisateurs amènent leurs propres appareils et applications mobiles, ils accroissent encore la diversité de l'environnement, et contournent les processus de la DSI. Dès lors, celle-ci ne peut pas compter sur la standardisation et le verrouillage des terminaux et de leurs applications pour sécuriser les données en mobilité.
Sécuriser les données en mobilité nécessite de comprendre ce que chaque système d'exploitation mobile peut ou ne peut pas faire. Les administrateurs peuvent alors pleinement tirer parti des technologies, applications et réglages supportés. Par exemple, la plupart des systèmes d'exploitation mobiles actuels supportent l'isolation native des applications – ou sandboxing –, et intègrent des capacités avancées de sécurisation du noyau.
Le support du chiffrement natif à l'échelle du terminal et de l'effacement à distance, varie toutefois. Pour cela, il est fréquent que les DSI choisissent une approche de sécurisation des données en mobilité en deux temps : elles commencent par établir et faire respecter des critères d'acceptation minimum, puis comblent les limitations des plateformes avec des outils tiers.

Déterminer quels terminaux accepter
Pour établir les critères d'acceptation des terminaux, il convient d'examiner l'architecture de sécurité de chaque plateforme pour étudier à quel point les applications utilisateur, opérateur et constructeur sont isolées les unes des autres, et du noyau du système d'exploitation.

Il convient également de savoir si les applications peuvent lire ou modifier les données d'autres applications et services en dehors du bac à sable – des fichiers partagés ou des messages, par exemple. L'examen doit également couvrir les permissions qui sont accordées – par défaut ou explicitement – aux applications, ainsi que le degré de contrôle que la DSI peut exercer pour détecter et bloquer des applications potentiellement dangereuses.
Comme leurs homologues pour le poste de travail, les systèmes d'exploitation mobiles souffrent de vulnérabilités susceptibles de mettre en danger les données. La question des mises à jour des applications et du système d'exploitation, leur délai de mise à disposition, s'avère particulièrement problématique dans un écosystème fragmenté.
La même considération s'applique à la provenance des applications mobiles. Le contrôle exercé par Apple s'avère efficace pour limiter la diffusion de logiciels malveillants pour iOS – sans toutefois l'empêcher complètement. C'est un facteur à prendre en compte dans l'établissement des critères d'acceptabilité. Par exemple, certaines entreprises interdisent les terminaux Android, ou n'en autorisent que certaines versions.
Pour beaucoup, les critères de base non négociables touchent à une version d'OS mobile minimum, le support matériel du chiffrement complet du terminal, des interfaces d'administration OTA, la possibilité d'imposer l'utilisation d'un mot de passe robuste, celle d'effacer le terminal à distance, d'enregistrer les activités, de détecter les opérations de jailbreak ou de rootage, voire de gérer dans une certaine mesure les applications installées. Les terminaux ne répondant pas à ces critères de base sont susceptibles d'être interdits d'accès aux réseaux et services de l'entreprise, ou bien autorisés dans une mesure limitée qui ne mette pas en danger les données.

Protection native des données : une base
Les smartphones et les tablettes sont appelés à être perdus, avec les données métiers qu'ils transportent. Le chiffrement complet du terminal peut souvent empêcher un appareil perdu d'être à l'origine d'une brèche de données.
Mais un tel chiffrement peut s'avérer d'une portée limitée sur certaines plateformes. Par exemple, l'effacement à distance est supporté par tous, mais son efficacité varie. Sur les appareils Apple et BlackBerry, les clés de chiffrement sont supprimées, ce qui rend les données chiffrées irrécupérables. Sur les anciens appareils Android sans chiffrement matériel, l'effacement n'est qu'une réinitialisation en conditions de sortie d'usine. Ce qui est susceptible de laisser les données exposées en cas de perte, de vol ou de revente du terminal.
De la même manière, un système de fichiers chiffré ne peut pas pleinement sécuriser les données sur un terminal compromis. Il ne peut pas non plus empêcher les utilisateurs de déplacer des données sur des emplacements non chiffrés. Lorsque des applications professionnelles et personnelles coexistent sur un même appareil, il y a plus de chances pour qu'une application malicieuse ou trop curieuse compromette des données d'entreprise présente sur le même système de fichiers. A moins que la DSI ne prenne des mesures préventives, un employé autorisé à accéder à un terminal chiffré peut aisément laisser fuir des données par e-mail ou transfert vers un service de stockage en mode Cloud.
La protection native des données en mobilité apparaît en fait comme un point de départ essentiel, mais pas suffisant. Pour profiter pleinement de ce que peuvent offrir les systèmes d'exploitation mobiles modernes, il convient d'utiliser une solution de gestion de la mobilité d'entreprise (EMM) pour enrôler les appareils acceptables et provisionner leurs réglages, en commençant par des points tels que la robustesse du mot de passe, le recours au lecteur d'empreintes digitales, ou encore le nombre de tentatives autorisées. Une authentification robuste est critique parce que des codes PIN faciles à deviner peuvent neutraliser un chiffrement fort. Il convient aussi d'activer l'effacement à distance et de recueillir le consentement explicite de l'utilisateur durant l'enrôlement à l'invocation de cette fonctionnalité en cas de dernier recours, et dans des conditions très précises.
Article original de Lisa Phife

Réagissez à cet article

Original de l’article mis en page : Trois étapes pour mieux protéger les données en mobilité

Pourquoi l’inventeur du Web rêve d’un autre Internet ?

Pourquoi l’inventeur du Web rêve d’un autre Internet ?

Inventeur du Web il y a plus de 25 ans, Tim Berners-Lee regrette le pouvoir quont pris sur lui les états et les grandes entreprises comme Google ou Facebook. Il souhaite pousser vers un Web plus déconcentré et plus sûr pour ses utilisateurs.

Mais qu'a-t-on fait d'Internet ? C'est la question que se posent régulièrement des pionniers du Web, qui rêvaient de changer le monde et qui l'ont effectivement fait, sans toujours bien savoir si c'est pour le meilleur ou pour le pire. Internet a apporté son lot incontestable d'améliorations dans la vie sociale, en permettant aux citoyens de s'informer davantage, de partager des connaissances et d'entrer plus facilement en contact les uns avec les autres. Mais il est aussi devenu un moyen inédit de surveillance de la population, et une machine libérale qui favorise les plus gros dans une économie plus que jamais mondialisée.
Parmi ceux qui semblent avoir quelques regrets figure l'inventeur du World Wide Web, Tim Berners-Lee. L'homme, qui a créé la première page Web il y a plus d'un quart de siècle, s'est désolé dans le New York Times de ce qu'était devenu en partie Internet. « Il contrôle ce que les gens voient, crée des mécanismes sur la manière dont les gens interagissent. Ce fut génial, mais l'espionnage, le blocage de sites, le détournement du contenu des gens, vous faire aller sur les mauvais sites web… tout ça mine complètement l'esprit d'aider les gens à créer », condamne-t-il.

NOUS N'AVONS PAS UN PROBLÈME TECHNOLOGIQUE, NOUS AVONS UN PROBLÈME SOCIAL

Berners-Lee voit un problème majeur dans le développement du Web qu'il a créé ; la possibilité pour les états ou de grandes entreprises de prendre le contrôle et d'imposer leur puissance. Pour les états, il s'agit par exemple de la possibilité qu'ils ont de bloquer l'accès à des sites internet (comme c'est désormais fréquent en France), ou de traquer les communications pour identifier ou géolocaliser des dissidents. Concernant les entreprises, le souci est davantage dans le pouvoir immense que des Facebook ou Google ont sur les populations du monde entier, en étant les principaux vecteurs d'informations, et en glanant des informations de plus en plus précises sur les habitudes et les pensées de chacun.

Pour défendre l'idée de repenser Internet, l'ingénieur a donc participé cette semaine à la conférence Decentralized Web Summit de San Francisco, organisée notamment par la fondation Internet Archive, et des acteurs impliqués dans le bitcoin et la blockchain. Mais il prévient que la solution ne sera pas seulement technique. « Le Web est déjà décentralisé », rappelle-t-il. « Le problème c'est la domination d'un moteur de recherche, d'un grand réseau social, d'un Twitter pour le microblogging. Nous n'avons pas un problème technologique, nous avons un problème social ».
« Nous sommes au bord de découvrir qu'une entreprise peut en arriver au point où en réalité elle contrôlera tout ce que chacun d'entre nous voit », s'était déjà inquiété Berners Lee dans une interview à GeekWire. « Elle décidera des posts de ses amis et des articles de journaux qu'une personne voit, et nous réalisons que nous parlons d'une seule grande multinationale qui a soudainement le contrôle complet sur la perception qu'a quelqu'un de la planète sur laquelle il habite. C'est une bataille constante et nous en sommes très proches tout le temps ».

UN PAIEMENT PLUS FLUIDE POUR UN INTERNET PLUS SAIN

Pour aider à réinventer le Web, Tim Berners-Lee rêve notamment d'un réseau social respectueux de la vie privée des utilisateurs et de leur liberté d'expression. Il est membre du conseil d'administration de MeWe, qui se rêve en Facebook éthique. D'autres technologies décentralisées peuvent aussi aider, comme Tor bien sûr, mais aussi des initiatives comme ZeroNet, qui prétend héberger un Web non censurable en utilisant BitTorrent et du chiffrement, ou MaidSafe, qui utilise aussi une architecture P2P et un système d'échange monétaire baptisé SafeCoin.
À cet égard, Tim Berners-Lee espère aussi voir prospérer un Web où le paiement électronique serait beaucoup plus aisé, et sans intermédiaires à qui verser des commissions (ce qui était à l'origine l'idée du bitcoin, même s'il manque de fluidité dans la validation des transactions). « Imaginez un monde où le fait de payer pour des choses serait facile des deux côtés », demande-t-il, en faisant remarquer que « le modèle publicitaire est le seul modèle pour trop de gens sur le web actuellement ».
Les journaux, par exemple, devraient pouvoir proposer de faire payer quelques centimes pour lire un article, ce qui rapporterait davantage que la publicité, offrirait davantage d'espace d'affichage pour l'information, et éviterait de tracer l'internaute. Or aujourd'hui, le jeu des commissionnements et des empilements d'intermédiaires fait qu'il est pratiquement impossible d'avoir sur internet la fluidité de paiement offerte par l'argent liquide.
Crédit photo de la une : CC Kristina D.C. Hoeppner
Article original de Guillaume Champeau

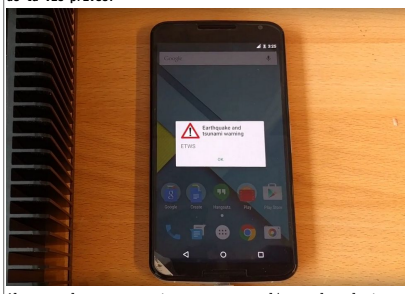
Original de l'article mis en page : Pourquoi linventeur du Web rêve dun autre Internet — Politique — Numerama

---

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

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 : Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse