Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

---

Obligation de résultat de la part d’un éditeur de logiciels. Autre cas d’école

Obligation de résultat de la part d’un éditeur de logiciels. Autre cas d’école

---

Le tribunal de commerce de Nanterre a condamné le groupe d'assurance mutualiste à verser plus de 1,4 million d'euros à l'éditeur et intégrateur d'un progiciel métier.
La Mutuelle assurance des commerçants et industriels de France et des cadres et salariés de l'industrie et du commerce (Macif) n'a pas obtenu gain de cause. Dans un jugement du 24 juin 2016 repéré par Legalis, le tribunal de commerce de Nanterre (Hauts-de-Seine) l'a condamnée pour résiliation abusive d'un contrat d'intégration et du contrat de licence et de maintenance associé.

Contrat d'intégration mal ficelé
En 2012, la Macif a lancé un appel d'offres pour doter sa filiale Macifilia d'une nouvelle solution de gestion d'assurance IARD (incendie, accidents et risques divers). L'éditeur et intégrateur IGA Assurance l'a remporté. C'est au terme d'un contrat de cadrage destiné à préciser le périmètre fonctionnel de son progiciel (ERP) Veos, que les parties ont conclu, le 8 février 2013, un contrat d'intégration d'un montant forfaitaire supérieur à 4 millions d'euros hors taxes.
Parallèlement, un contrat de licence et de maintenance a été signé. Mais à la suite d'échanges multiples, de retards et de modifications de planning, la Macif met en demeure, le 23 juillet 2013, IGA de livrer toutes les spécifications fonctionnelles détaillées (SFD) de la V1 (sur quatre prévues) sous 30 jours. IGA indique, le mois suivant, que 62 SFD sur 75 ont été livrées… Considérant qu'IGA n'a pas respecté le délai imparti et que la moitié des besoins exprimés ont été couverts, la Macif prononce en septembre 2013 la résiliation du contrat pour faute grave et répétée d'IGA. Le prestataire a contesté.
À la demande de la Macif, le tribunal de commerce a donc nommé un expert judiciaire pour clarifier le cadre contractuel sur lequel s'oppose l'assureur et son prestataire. Dans son rapport, l'expert a notamment indiqué que « la Macif était contractuellement responsable de la validation de l'exhaustivité des SFD, mais que IGA aurait dû vérifier l'exhaustivité ou la suivre et la gérer avec la Macif ».

Adapter ses processus à l'outil
C'est dans ces circonstances que la Macif a assigné son prestataire, en juin 2015, pour tenter d'obtenir la résolution judiciaire des contrats du 8 février 2013 aux torts d'IGA Assurance. Mais le tribunal ne l'a pas suivie, bien au contraire. Selon lui, « en faisant le choix de la solution progicielle Veos à l'issue d'une phase préalable d'analyse comparative, la Macif a nécessairement entendu adapter majoritairement ses modes de fonctionnement et ses processus au nouvel outil et non l'inverse ».
Dans ce contexte, l'obligation de résultat se limitait aux développements et aux adaptations à apporter à la version standard du progiciel. Le contrat n'imposant pas au prestataire de livrer des spécifications détaillées pour l'ensemble des besoins exprimés par la Macif. Le tribunal de commerce a donc prononcé la résolution des contrats du 8 février 2013 aux torts de la Macif et l'a condamnée.
Le groupe d'assurance mutualiste devra verser 1,14 million d'euros de dommages et intérêts à l'éditeur et intégrateur du progiciel : la SARL IGA Assurance. Et lui régler 276 120 euros pour une facture impayée de septembre 2013, plus 226 190 euros au titre des frais de justice.
Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : La Macif condamnée pour rupture abusive de contrat d’intégration

---

Directive européenne sur la sécurité des réseaux et des systèmes d’information

	Directive européenne sur la sécurité des réseaux et des systèmes d’information

---

Les entreprises qui fournissent des services essentiels, par exemple l'énergie, les transports, les services bancaires et de santé, ou numériques, tels que les moteurs de recherche et les services d'informatique en nuage, devront améliorer leur capacité à résister à des cyber-attaques, selon les premières règles de cybersécurité à l'échelle européenne, approuvées par les députés mercredi.

L'établissement de normes de cybersécurité communes et renforcer la coopération entre les pays de l'Union aidera les entreprises à se protéger elles-mêmes, et aussi à prévenir les attaques contre les infrastructures interconnectées des pays européens, estiment les députés.

« Des incidents de cybersécurité possède très souvent un aspect transfrontalier et concernent donc plus d'un État membre de l'Union européenne. Une protection fragmentaire de la cybersécurité nous rend tous vulnérables et pose un risque de sécurité important pour l'Europe dans son ensemble. Cette directive établira un niveau commun de sécurité de réseau et d'information et renforcera la coopération entre les États membres. Cela contribuera à prévenir à l'avenir les cyberattaques sur les infrastructures interconnectées européennes importantes », a déclaré le rapporteur du Parlement Andreas Schwab (PPE, DE).

La directive européenne sur la sécurité des réseaux et des systèmes d'information « est également l'un des premiers cadres législatifs qui s'applique aux plates-formes. En phase avec la stratégie du marché unique numérique, elle établit des exigences harmonisées pour les plates-formes et veille à ce qu'elles puissent observer des règles similaires quel que soit l'endroit de l'Union européenne où elles opèrent. C'est un énorme succès et une première étape importante vers l'établissement d'un cadre réglementaire global pour les plates-formes dans l'Union », a-t-il ajouté.

Les pays de l'UE devront lister les entreprises de « services essentiels »
La nouvelle législation européenne prévoit des obligations en matière de sécurité et de suivi pour les « opérateurs de services essentiels » dans des secteurs tels que ceux de l'énergie, des transports, de la santé, des services bancaires et d'approvisionnement en eau potable. Les États membres de l'UE devront identifier les entités dans ces domaines en utilisant des critères spécifiques, par exemple si le service est essentiel pour la société et l'économie, et si un incident aurait des effets perturbateurs considérables sur la prestation de ce service.

Certains fournisseurs de services numériques – les marchés en ligne, les moteurs de recherche et les services d'informatique en nuage – devront aussi prendre des mesures pour assurer la sécurité de leur infrastructure et devront signaler les incidents majeurs aux autorités nationales. Les exigences de sécurité et de notification sont, cependant, plus légères pour ces fournisseurs. Les micro- et petites entreprises numériques seront exemptées de ces exigences.

Mécanismes de coopération à l'échelle européenne
Les nouvelles règles prévoient un « groupe de coopération » stratégique pour échanger l'information et aider les États membres à renforcer leurs capacités en matière de cybersécurité. Chaque pays de l'Union devra adopter une stratégie nationale relative à sécurité des réseaux et des systèmes d'information.

Les États membres devront aussi mettre en place un centre de réponse aux incidents de sécurité informatique (CSIRT) pour gérer incidents et risques, discuter des questions de sécurité transfrontalière et identifier des réponses coordonnées. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) jouera un rôle clé dans la mise en œuvre de la directive, en particulier en matière de coopération. La nécessité de respecter les règles de protection des données est réitérée tout au long de la directive.

Prochaines étapes
La directive sur la sécurité des réseaux et des systèmes d'information sera bientôt publiée au Journal officiel de l'Union européenne et entrera en vigueur le vingtième jour suivant sa publication. Les États membres auront alors 21 mois pour transposer la directive dans leur législation nationale et six mois supplémentaires pour identifier les opérateurs de services essentiels.

Directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Procédure: codécision, seconde lecture
Source : Parlement européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité: les députés soutiennent les règles pour aider les entreprises de services clés à… – Linkis.com

---

Sanction de la CNIL pour BrandAlley.fr

Sanction de la CNIL pour BrandAlley.fr

La CNIL vient d'infliger une sanction administrative de 30 000 euros à l'encontre de BrandAlley.fr. La société éponyme, derrière ce site de ventes en ligne, est épinglée pour plusieurs indélicatesses à l'égard de la loi de 1978.

Le 13 janvier 2015, une délégation de la CNIL effectuait un premier contrôle sur place pour relever déjà différents manquements de cette société française. Cela aurait pu en rester là si tout avait été rectifié à temps, mais en mars de la même année, une cliente a saisi la CNIL pour se plaindre de difficultés dans l'exercice de son droit d'accès aux données personnelles. Cette internaute adressait d'ailleurs au site de e-commerce une nouvelle lettre en mai 2015, sans plus d'effet.
Le 3 juillet 2015, BrandAlley était du coup mise en demeure par la CNIL de corriger plusieurs points de son système dans les trois mois. Bon prince, la Commission lui accordait un peu plus tard une rallonge de trois nouveaux mois. Les points litigieux visent à :
• Encadrer le traitement relatif à la prévention des fraudes,
• Mettre en place d'une durée de conservation des données clients,
• Recueillir le consentement préalable des clients pour la conservation des données bancaires,
• Prendre en compte de la demande de la plaignante,
• Obtenir l'accord des internautes s'agissant des cookies,
• Cesser de transmettre les données à caractère personnel vers des pays hors UE qui n'assurent pas un niveau suffisant de protection de la vie privée et des libertés et droits fondamentaux.

Dans un courrier de janvier 2016, BrandAllay affirmait à la CNIL qu'elle s'était désormais mise en conformité. Peu satisfaite des réponses « lacunaires », la Commission organisait un nouveau contrôle sur place en février 2016. Contrôle qui a montré la persistance de plusieurs problèmes déjà relevés. En outre, un mois plus tard, elle a effectué un contrôle à distance du site Internet, une possibilité accordée par la loi sur la consommation.
La procédure gagnait alors un tour de vis supplémentaire. La CNIL a désigné un rapporteur, en l'occurrence François Pellegrini, une étape préalable à toute sanction où la société peut encore donner ses explications. Dans ce document désormais public , le rapporteur a constaté plusieurs défauts.

Des réactions trop tardives

Premièrement, BrandAllay.fr n'avait pas déposé dans le délai imparti, de demande d'autorisation pour la mise en œuvre d'un traitement antifraude. Selon les éléments du dossier, c'est « la réception du rapport de sanction qui a conduit la société à effectuer une demande d'autorisation ». Mais beaucoup trop tardivement pour ne pas abuser de la patience de l'autorité administrative…
S'agissant de la durée de conservation des données personnelles, on se retrouve un peu dans même situation. À l'échéance du délai imparti, la société avait indiqué s'être conformé à la norme simplifie 48, celle relative à la gestion de clients et de prospects. Dans le même temps, elle ajoutait que les données clients seraient conservées 5 années durant, à compter de la fin de la relation commerciale. Or ce délai non prévu par la norme en question. Pire, lors du deuxième contrôle sur place, la CNIL a constaté qu' « aucune purge des données n'avait été réalisée ». Les explications fournies par le site de e-commerce – liées à la complexité de mise en œuvre – n'ont pas eu de poids, même si elle a depuis corrigé le tir pour revenir à un délai de conservation de 3 ans.

Cookies, chiffrement, Maroc et Tunisie

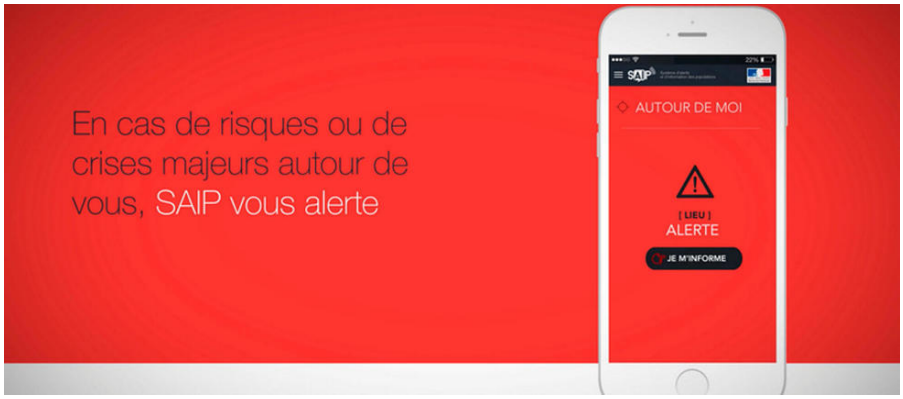
S'agissant des cookies, la société mise en demeure avait informé l'autorité de la mise en place un bandeau afin de recueillir le consentement des internautes, avant dépôt de cookies. Le contrôle en ligne effectué en mars 2016 a révélé la solidité de cette affirmation. D'un, le fameux bandeau « était rédigé de telle sorte qu'il n'informait pas les utilisateurs de leur possibilité de paramétrer le dépôt de cookies ». Soit un joli manquement à l'article 32-II de la loi de 1978.
De deux, des cookies à finalités publicitaires étaient déposés dès l'arrivée sur le site, sans l'ombre d'un consentement préalable. Pour ce dernier point, la CNIL n'a finalement pas retenu de grief, s'estimant « insuffisamment éclairée (…) sur la répartition exacte des responsabilités entre l'éditeur du site, les annonceurs et les régies publicitaires concernés ». Par constat d'huissier, BrandAlley a par ailleurs démontré s'être mise depuis d'aplomb.
Ce n'est pas tout. La CNIL a pareillement dénoncé l'absence de chiffrement du canal de communication et d'authentification lors de l'accès à BrandAlley.fr (usage du HTTP, plutôt que HTTPS). Le 29 mars 2016, la société a produit un nouveau constat d'huissier pour montrer à la CNIL que ce défaut se conjuguait désormais au passé. Un peu tard là encore pour la Commission qui a relevé un nouveau manquement.
Enfin, la société transférait vers le Maroc et la Tunisie les données personnelles de ses clients, via l'un de ses sous-traitants. Malgré des affirmations en sens contraire en janvier 2016, la CNIL a relevé en février la persistance de ces transferts. Or, en principe, de telles opérations ne sont possibles que si le pays de destination offre un niveau de protection comparable à celui en vigueur en Europe, ce qui n'était pas le cas ici (pas plus qu'aux Etats-Unis depuis l'invalidation du Safe Harbor par la justice européenne).
Après délibération, la CNIL a décidé de sanctionner la société de 30 000 euros d'amende, outre de rendre public la délibération. Une sanction loin d'être négligeable, le critère de la confiance sur Internet étant cruciale pour un site de e-commerce. La société peut maintenant attaquer, si elle le souhaite, la décision devant le Conseil d'État.

Article original de Marc Rees

Réagissez à cet article

Original de l’article mis en page : Données personnelles : BrandAlley.fr sanctionné par la CNIL

Attentat à Nice : l’application « alerte attentat » sur la sellette



Attentat à Nice : l’application « alerte attentat » sur la sellette

---

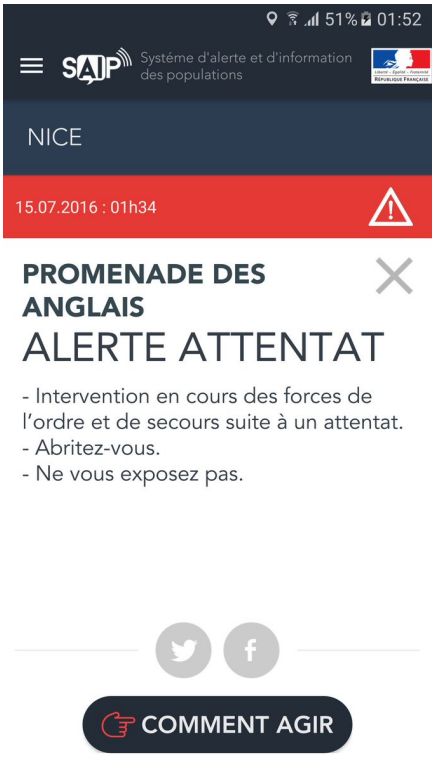
Le dispositif mis en œuvre par le ministre de l'Intérieur, censé prévenir les populations locales d'un attentat en cours, a failli. Les critiques pleuvent.

Chou blanc. L'application SAIP (Système d'alerte et d'information aux populations) « alerte attentat » avait été lancée par le ministre de l'Intérieur, Bernard Cazeneuve, avant l'Euro 2016 de football afin d'informer en temps réel les populations concernées de l'imminence d'une attaque. Hier, elle a tardé à fonctionner à Nice, au moment où le camion meurtrier faisait un carnage sur la promenade des Anglais. Ce dispositif aurait dû s'activer dans les quinze minutes qui ont suivi cet attentat, mais il n'en a rien été.

Les tweetos fustigent cet échec

Sur le réseau social Twitter, les internautes ont épinglé l'inefficacité et l'inutilité de ce système. Selon certains, l'alerte attentat, supposée prodiguer des conseils de survie en cas d'attaque, se serait déclenchée deux heures après le massacre de Nice, soit à un moment où la France entière était déjà informée du drame qu'elle venait de connaître.

Voir l'image sur Twitter



Suivre

Olivier Jaillet @OJaillet

Alerte #attentat sur #SAIP qui se déclenche 2 heures après le drame… Quel est l'utilité de l'application ?? #Nice

02:07 – 15 Juil 2016

•

•

1515 Retweets

•

22 j'aime

Voir l'image sur Twitter

Suivre

Jonathan Quique @jonathanquique

Première notification à 1h34, l'app #SAIP n'était pas prête …

07:16 – 15 Juil 2016

•

•

1 Retweet

•

11 j'aime

Il appartiendrait en fait au préfet du département concerné par un attentat de choisir de déclencher ou non l'alerte sur les smartphones des personnes ayant téléchargé l'application SAIP. On ignore encore si c'est le préfet des Alpes-Maritimes qui a décidé de ne pas faire fonctionner l'alerte, ou s'il s'agit d'un dysfonctionnement.

Article original de Emmanuel Ammar

Réagissez à cet article

Original de l’article mis en page : Attentat à Nice : l’application « alerte attentat » sur la sellette – Le Point

---

De nouvelles investigations sur l’IP Tracking en préparation

De nouvelles investigations sur l’IP Tracking en préparation

Les cybermarchands sont prévenus : la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) va mener « dans les prochains mois » de nouvelles investigations relatives à l'IP Tracking, cette technique de pistage dont aucun cas avéré n'avait été détecté lors d'une précédente enquête, remontant à 2013.

Certains sites de e-commerce modulent-ils leurs tarifs en fonction du nombre de visites de leurs utilisateurs ? C'est en tout cas ce que soutiennent de nombreuses personnes, au motif que le prix de certains articles augmenterait artificiellement en cas de consultations à répétition d'un même article. Le but : faire croire au consommateur que les biens restants (des billets d'avion ou des chambres d'hôtel par exemple) diminuent et qu'il faut donc passer commande sans tarder… Cette technique est généralement appelée « IP Tracking », dans la mesure où elle repose sur la reconnaissance de l'adresse IP de la connexion utilisée.

La pratique reste toutefois « *difficile à qualifier juridiquement et difficile également à démontrer* » selon Martine Pinville, la secrétaire d'État au Commerce. Interpellée par un sénateur qui lui avait transmis une question écrite en juillet 2015, l'intéressée rappelle que l'enquête menée à ce sujet en 2013 par la CNIL et la DGCCRF était ainsi arrivée à la conclusion qu' « *aucune des techniques observées ne prenait en compte l'adresse IP des internautes comme élément déterminant ou ne visait à moduler le prix des produits ou services proposés aux consommateurs* ».

Aucune plainte de consommateurs enregistrée par la DGCCRF

Pour l'heure, poursuit Martine Pinville, « *la DGCCRF n'a pas été saisie de plaintes de consommateurs concernant des pratiques « d'IP tracking »* ». Bercy n'aurait pas non plus « *eu connaissance de signalements de cette nature* » au sein du réseau de coopération administrative du « G29 » des CNIL européennes.

La secrétaire d'État cherche néanmoins à rassurer : elle annonce que « *le sujet de « l'IP tracking » fera l'objet dans les prochains mois de nouvelles investigations* » de la part de la DGCCRF. Si de telles pratiques venaient à être débusquées, les cybermarchands concernés pourraient être poursuivis pour pratiques commerciales déloyales ou trompeuses, explique Martine Pinville, car « *susceptible[s] d'altérer le comportement économique du consommateur* ». Les contrevenants s'exposeraient alors à des peines pouvant aller jusqu'à deux ans de prison et 300 000 euros d'amende.

Un front pourrait également s'ouvrir en matière de protection des données personnelles. « *L'adresse IP étant une donnée personnelle, il faudrait avant toute exploitation, demander l'accord et le consentement du consommateur ainsi que la déclaration de ces données à la CNIL, en respectant la procédure requise : durée de conservation des données, finalité, etc.* »

Article original de Xavier Berne

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 : IP Tracking : de nouvelles investigations de la répression des fraudes

---

Les mots de passe disparaîtront progressivement

d’ici 2025

Les mots de passe disparaîtront progressivement d’ici 2025

La technologie de biométrie comportementale et d’authentification à deux facteurs sont à la hausse comme des alternatives plus sûres, selon une étude.
Une étude de 600 professionnels en sécurité de l’opérateur de téléphonie mobile ID TeleSign a révélé que la protection du compte client est un souci majeur pour les entreprises, avec 72 % des personnes interrogées disant que les mots de passe seront éliminés progressivement d’ici à 2025. De plus en plus d’entreprises, selon le rapport, remplacent les mots de passe avec la biométrie comportementale et l’authentification à deux facteurs (2FA) avec 92 % des experts en sécurité affirmant que cela va améliorer la sécurité des comptes considérablement.
« La grande majorité des professionnels en sécurité ne font plus confiance aux mots de passe pour travailler », a déclaré Ryan Disraeli de TeleSign parce que 69 % des répondants ont dit qu’ils ne pensent pas que les noms d’utilisateur et mots de passe fournissent assez de sécurité. Les prises de contrôle de compte (ATO) étaient une préoccupation majeure pour 79 %, alors que 86 % sont préoccupés par l’authentification ID d’identité des utilisateurs du web et des applications mobiles avec 90 % étant touchées par des fraudes en ligne l’an dernier.
Plus de la moitié (54 %) des organisations disent qu’ils passeront à la biométrie comportementale en 2016 ou plus tard tandis que 85 % ont dit qu’ils mettraient en œuvre le 2FA dans les 12 prochains mois. Huit des 10 répondants croient que la biométrie comportementale ne dégradera pas l’expérience utilisateur.
Lire l’étude complète ici
https://iatranshumanisme.files.wordpress.com/2016/07/telesign-report-beyond-the-password-june-2016-1.pdf
Article original de Jaesa

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 : Les mots de passe disparaîtront progressivement d’ici 2025 | Intelligence

Huit bonnes pratiques pour bien sécuriser les objets connectés

Huit bonnes pratiques pour bien sécuriser les objets connectés

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Le point.

Gartner prédit 26 milliards d'objets connectés d'ici 2020. En 2016 ce sont 4,9 milliards de dispositifs connectés qui devraient être déployés. Des objets qui seront potentiellement confrontés à un grand nombre d'attaques. En effet, le volume des cyber-attaques recensé par l'étude The Global State of Information Security® Survey 2016, réalisée par le cabinet d'audit et de conseil PwC en collaboration avec CIO et CSO, a progressé de 38 % dans le monde en 2015. Comment alors sécuriser au mieux ses objets connectés ?

En appliquant quelques bonnes pratiques.

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Plusieurs zones « sensibles » sont donc à surveiller au sein des objets connectés notamment au niveau du capteur et au niveau du transfert des données.

Pour le capteur, l'un des moyens les plus efficaces pour se protéger consiste à sécuriser le hardware grâce à un Secure Element, qui empêche tout accès à l'information lorsqu'on se connecte au capteur. Un élément sécurisé repose sur une plate-forme matérielle inviolable qui héberge des données, cryptées ou non, en toute sécurité et en conformité avec les règles de sécurité fixées par les autorités de confiance. Certains de ces éléments, comme les cartes microSD, peuvent même être amovibles.

Pour sécuriser les données, il est indispensable d'utiliser des technologies de chiffrement robustes afin de lutter contre le piratage ou les interceptions. En effet, le chiffrement rend les données impossibles à lire pour qui ne possède pas la clé de déchiffrement de 128 bits ! Efficace pour repousser les hackers même les plus coriaces.

Une fois le capteur protégé et les données chiffrées, il est important d'assurer la sécurité de l'information lors de son transfert de bout en bout : du capteur jusqu'au portail client.

L'utilisation d'un système de clés multiples géré par un tiers de confiance tel que le propose le protocole LoRa s'avère une solution des plus fiables.

Un tiers de confiance fournit un système de gestion de clé – Key Management System (KMS) – qui permet de générer une AppKey unique pour chaque capteur. A chaque nouvelle session, une AppSKey – Application Session Key – dérivée de l'AppKey sert au chiffrement des données du client. L'opérateur n'a pas accès à ces 2 clés, elles ne sont connues que du tiers de confiance dans le KMS et du client bien sûr pour déchiffrer les données.

Une fois les données récupérées, l'utilisation d'un VPN est bien sûr conseillé.

En agissant à ces différents niveaux, vous appliquez une sécurité optimale à vos objets connectés. De plus, vous pouvez appliquer quelques conseils pour assurer une sécurité de bout en bout des processus :

1. Évaluez le bon degré de sécurité sur le capteur en fonction de la criticité de la donnée : selon l'information concernée, il n'est pas forcément nécessaire d'insérer un Secure Element dans le capteur.
2. Utilisez une technologie avec un protocole de chiffrement robuste de type AES128 par exemple.
3. Mettez en place des infrastructures intégrant l'état de l'art en termes de chiffrement.
4. N'écrivez pas vos clés de cryptage sur disque dur : privilégiez les éléments de sécurité non stockés et volatiles. Calculées « à la demande » par un algorithme, elles ne peuvent donc pas être piratées en cas d'attaque sur la base de données.
5. Optez pour un renouvellement de la clé de chiffrement à chaque connexion du capteur sur le réseau. Une clé renouvelée régulièrement à moins de risque d'être piratée.
6. Utilisez un portail sécurisé pour accéder à vos données applicatives chiffrées : vous avez ainsi, seul, la possibilité de déchiffrer les données. Toutefois, si vous choisissez de ne pas les déchiffrer vous-même, assurez-vous que votre prestataire le fasse sur un cloud sécurisé.
7. Choisissez des technologies en perpétuelle évolution : au sein de la LoRa Alliance, un groupe dédié fait évoluer en permanence le protocole afin d'être toujours à la pointe de la sécurité.
8. Optez pour un opérateur qui intègre les processus de sécurité recommandés par l'ANSSI dans la conception et l'exploitation de son réseau.

Article original de Franck Moine

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.

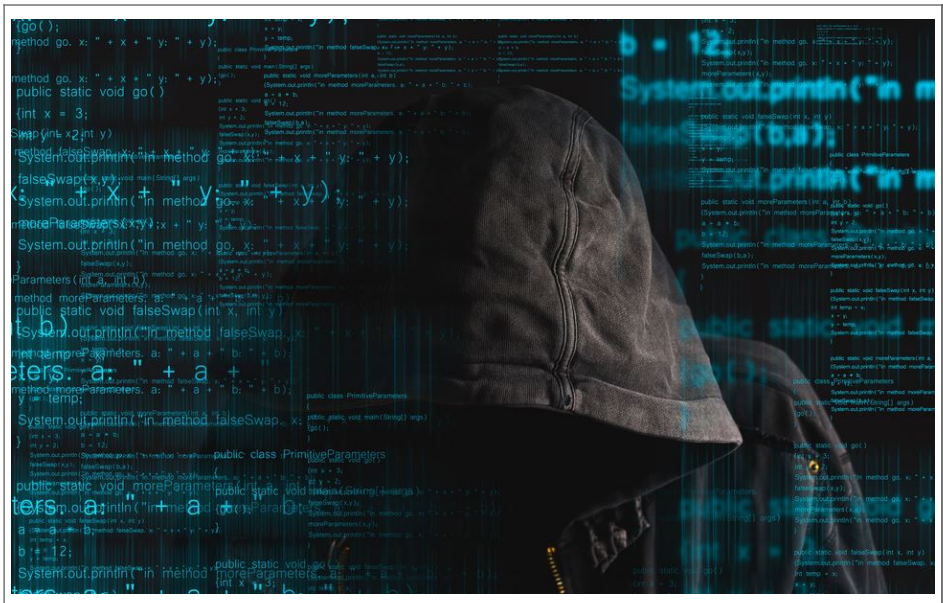
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Huit bonnes pratiques pour bien sécuriser les objets connectés – JDN

Un cousin du malware Furtim cible les énergéticiens européens



Un cousin du malware Furtim cible les énergéticiens européens

---

SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG. L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de Furtim cible les énergéticiens européens

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc a-t-il les capacités de se transformer en « Silicon Valley » du Maghreb? Hamza Hraoui, conseiller en communication d'influence pour les entreprises et les dirigeants, estime que »oui ».

Dans un entretien paru jeudi 7 juillet au HuffpostMaroc, cet expert estime que le Maroc a toutes les potentialités pour cet objectif, à condition de revoir le fonctionnement de l'Agence nationale de réglementation des télécommunications (ANRT). »Nous sommes en tout cas crédibles et légitimes pour être le spot technologique de la région », souligne t-il. »Le taux de pénétration d'internet dépasse 56% chez nous alors qu'en Tunisie c'est 44%, en Algérie c'est moins de 20%. En plus d'avoir la population la plus connectée du Maghreb, le Maroc connaît également le plus fort dynamisme de ses médias en ligne. » En outre, le Maroc a pris de l'avance sur le plan des infrastructures de TIC, selon lui: » quand l'Algérie a introduit la 3G qu'en 2013, nous avons aujourd'hui la couverture 4G la plus large du Maghreb. » Mais, tempère l'expert, le pays accuse déjà un retard dans ce domaine.

Le »Hic »

»Au Maroc on est au point mort », affirme t-il, avant d'expliquer que »si la stratégie industrielle (du Ministre de l'Industrie et de l'Economie numérique) a esquissé les grandes lignes de l'économie numérique du pays, la structuration des écosystèmes numériques tarde à venir », même si »le potentiel est là. » Pour Hamza Hraoui, »il faut enclencher maintenant notre transformation et prendre le train de la nouvelle économie en misant sur notre tissu entrepreneurial. » Car »les Marocains attendent un vrai plan du numérique, conquérant et volontariste qui permettra d'accompagner les projets structurants des entreprises sur les marchés, où le Maroc peut acquérir d'ici 3 à 5 ans, un leadership continental: fabrication additive comme les imprimantes 3D, les objets connectés, la réalité augmentée, les villes intelligentes, les écoles du numérique… » Pour cela, il faut que bien des barrières tombent, et que les opérateurs du secteur rattrapent le retard accusé par le Maroc dans le digital et l'économie numérique.

Faire sauter les barrières

Et, surtout, libérer le secteur des »interdits » et des blocages. Il estime ainsi que la Maroc, en interdiction de la VoiP, »donne un mauvais signal aux acteurs de la nouvelle économie suite à cette interdiction. » »Et ses répercussions se feront sentir à moyen et à long terme », ajoute cet expert en communication, qui appelle l'ANRT à faire »son update ». Plus direct, il accuse l'ANRT de cloisonner le secteur des TIC et empêcher l'économie numérique de se développer. »A l'heure du décloisonnement de l'information, de l'explosion de la data et de l'émergence de l'économie collaborative, l'ANRT poussée et pressée par les opérateurs télécom, nous a montré qu'elle vit encore à l'âge de pierre en enlevant aux jeunes étudiants, aux chercheurs, aux start-upers qui créent de la richesse dans ce pays l'essence même du progrès: le droit à la mobilité. » Pour lui, »cela nous montre à quel point nos institutions ont du mal à admettre que la relation public-autorité et l'ordre établi sont profondément bouleversés par le digital, obligeant les hommes politiques à revoir en profondeur leurs messages, décisions et façons de faire. » A fin décembre 2015, le Maroc comptait 13,89 millions d'abonnés à l'Internet fixe, soit un taux de pénétration de 41,1 %, alors que le parc de l'internet mobile compte 12,81 millions d'abonnés avec une progression de 69,58% par an.

Article original de Amin Fassi-Fihri

Réagissez à cet article

Original de l'article mis en page : TIC: Le Maroc peut créer une Silicon Valley au Maghreb, mais…(Expert) – Maghreb Emergent