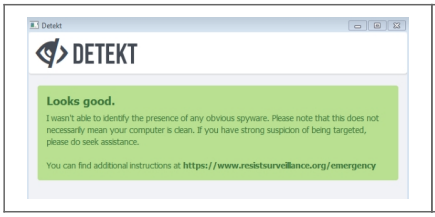
Déception : on a testé Detekt, il ne s’est rien passé



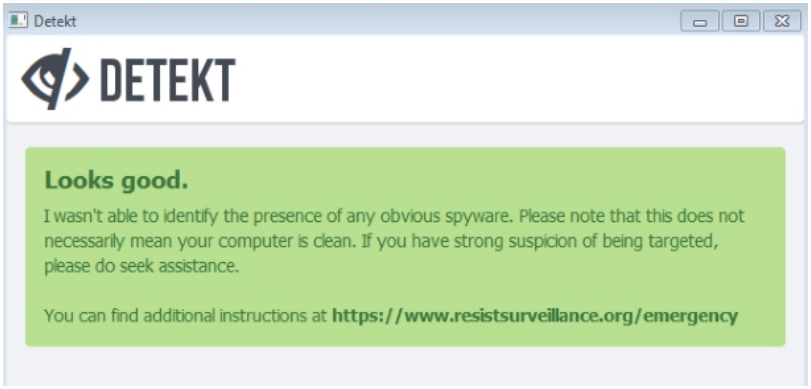
Déception : on a testé Detekt, il ne s’est rien passé

La promesse était belle : Detekt scanne votre ordinateur à la recherche des logiciels espions qui ciblent les activistes de tout poil, les minorités religieuses, et les journalistes. Nous avons essayé. Ça semble marcher, mais on est un peu amer.

Développé pendant deux ans par Claudio Guarnieri (un informaticien basé à Berlin) en partenariat avec Amnesty International et l'EFF entre autres, Detekt est un logiciel gratuit dont la promesse est d'informer l'utilisateur sur les spyware qui se seraient potentiellement glissés dans sa machine.

« Les défenseurs des droits de l'homme, les journalistes, les ONG, les opposants politiques, les minorités religieuses ou ethniques » sont particulièrement ciblés par les agences de renseignement qui utilisent des outils numériques d'espionnage, avertit l'auteur du logiciel.

La rédaction s'est donc prêtée au jeu du test. Après tout, savoir être espionné par la NSA, la DGSE ou Kim Jong-un, ça crédibilise notre travail.



(Personne ne nous espionne)

Après un scan offline de la machine, le verdict tombe. Rien de suspect sur l'ordinateur utilisé pour rédiger cet article. D'où deux propositions qui nous chagrinent : nous n'entrons dans aucune des catégories espionnées sus-nommées, ou bien nous sommes totalement inoffensifs pour les dites agences de renseignement. Préférons dire que nous avons beaucoup de chance.

En cas de détection d'un danger, l'auteur de Detekt mentionne que le nettoyage reste à faire soi-même. Detekt avertit, mais ne soigne pas. Par ailleurs, s'il ne trouve rien, cela ne signifie pas nécessairement que l'ordinateur ne soit pas la cible d'un service espion, mentionne le site de Detekt (ndlr. ouf !).

Programmé en Python, Detekt recherche des chevaux de Troie de certaines familles, comme DarkComet RAT, XtremeRAT, BlackShades RAT, njRAT, FinFisher FinSpy, HackingTeam RCS, ShadowTech RAT et Gh0st RAT. L'acronyme RAT signifie ici Remote Access Trojans. Le fichier readme.md donne d'autres informations techniques.

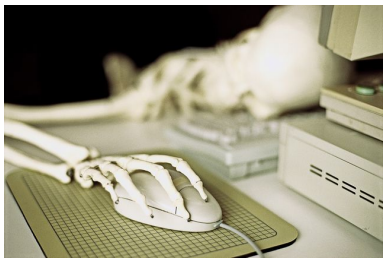
Au delà de cette annonce, qui est assurons-le une initiative salutaire, se pose la question de la pérennité de ce type de solution. Tout comme les antivirus, les anti spyware ne sont efficaces que s'ils sont régulièrement mis à jour, pour intégrer les nouvelles menaces, et celles déjà recensées, mais qui évoluent.

Et vous ? Vous en pensez quoi ?

Cliquez et laissez-nous votre avis…

Source : http://www.zdnet.fr/actualites/deception-on-a-teste-detekt-il-ne-s-est-rien-passe-39809965.htm

Technologie: Le numérique a la mort aux trousses



Technologie: Le numérique a la mort aux trousses

Aurore est décédée. C'était il y a cinq ans. Pourtant, son profil Facebook, lui, vit toujours. Ses proches l'ont transformé en mausolée. Untel poste une photo, un autre se fend d'un mot souvenir. Le tout ne serait pas choquant si le réseau social n'envoyait pas chaque année une alerte anniversaire à ses «amis». L'internaute ne meurt-il donc jamais?

Avec le développement des technologies digitales, la question de la mort numérique s'invite dans le débat, entraînant avec elle une foule de questions: que deviennent nos données numériques (mails, réseaux sociaux, photos…) lorsque l'on passe de vie à trépas? Peut-on hériter d'une bibliothèque iTunes comme on récupérait les vinyles de grand-père? Les morts du Web ont-ils le droit de reposer en paix? «Le sujet reste encore très peu encadré par la loi, souligne le conseiller national Jean Christophe Schwaab, c'est pourquoi j'ai décidé de déposer un objet parlementaire en septembre dernier, afin que le droit de succession s'intéresse enfin aux données numériques.» L'enjeu est de taille. Selon la Commission nationale de l'informatique et des libertés (Cnil), un profil Facebook sur cent – soit 130 millions de pages – appartiendrait à un mort.

Et vous ? Vous en pensez quoi ?
Cliquez et laissez-nous votre avis…

Obligation de résultat pour une agence de référencement de Sites Internet. Jurisprudence en vue ?

Obligation de résultat pour une agence de référencement de Sites Internet. Jurisprudence en vue ?

Par un jugement du 28 octobre 2014, le Tribunal de commerce de Paris a condamné un prestataire à rembourser son client pour n'avoir pas amélioré le référencement de son site.

Le tribunal a appliqué une clause du contrat de référencement par lequel le prestataire s'était engagé à atteindre « un positionnement minimum sur 50 % » des expressions clés convenues dans les deux premières pages des moteurs de recherche d'ici la fin de l'année de la prestation.

Or, le positionnement du site sur les moteurs de recherche avait diminué.
Le client avait donc demandé le remboursement du contrat, pour non respect de ses engagements.
Au contraire, le prestataire estimait que l'obligation de résultat prévue initialement au contrat s'était transformée en obligation de moyen, du fait d'un manque de collaboration du client.

Outre le fait que le contrat prévoyait bien un obligation de résultat, le Tribunal de commerce n'a pas suivit cette argumentation car il a estimé que le prestataire n'avait pas apporté la preuve que le client n'avait pas été suffisamment rapide et réactif. De plus, le Prestataire ne s'était jamais plaint du manque de rapidité et de collaboration du client lors de l'éxécution du contrat de référencement. Le Prestataire n'avait, par ailleurs, pas réagi au problème de lien retour que subissait le site, alors qu'il était connu depuis de nombreux mois.
Ce jugement rappelle de porter une attention toute particulière aux obligations du prestataire dans les contrats de référencement.
A partir du moment ou un clause est chiffrée, elle peut devenir une obligation de résultat et non une simple obligation de moyens…
Définitions :
Obligation de moyens :
L'obligation de moyens (Article 1137 du Code civil) est une obligation en vertu de laquelle le débiteur doit déployer ses meilleurs efforts pour atteindre l'objectif visé ; elle s'oppose à l'obligation de résultat, par laquelle un objectif est donné. Il s'agit d'une d'une appréciation site 'in abstracto', c'est-à-dire en référence à un modèle abstrait de « l'Homme raisonnable ».
La responsabilité du débiteur d'une obligation de moyens ne peut être engagée du seul fait qu'il n'a pas atteint un résultat (chiffré par exemple). Dans cette éventualité, c'est au créancier de démontrer que le débiteur n'a pas été assez diligent dans sa tentative d'exécution de son obligation.
Par contraste, la responsabilité du débiteur au titre d'une obligation de résultat pourra être engagée sur la simple constatation que le résultat convenu n'a pas été atteint. Le débiteur ne peut s'exonérer de sa responsabilité qu'en prouvant la survenance d'un cas de force majeure.

Obligation de résultat :
Obligation pour le débiteur d'atteindre un résultat précis.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.avocat-rainio.com/amelioration-du-positionnement-obligation-de-resultat-a-respecter.html

---

Quand chaque minute compte

Quand chaque minute compte..

McAfee, filiale d'Intel Security, publie aujourd'hui un nouveau rapport, « Prévention des menaces : chaque minute compte ! », qui évalue la capacité des entreprises à détecter et à détourner les attaques ciblées.

Ce dernier révèle également le Top 8 des indicateurs d'attaques les plus critiques et examine les meilleures pratiques proactives en matière de réponse aux incidents. Il illustre combien les entreprises sont plus efficaces lorsqu'elles effectuent des analyses des attaques subtiles en temps réel en prenant en compte plusieurs variables mais surtout dès lors qu'elles ont intégré et priorisé le temps de détection et les menaces intelligentes dans leur évaluation des risques.
Conjointement au rapport, une étude menée par Evalueserve, révèle que la majorité des entreprises interrogées manquent de confiance en leur capacité à détecter les attaques ciblées dans un temps opportun. Même les entreprises les mieux préparées à gérer les attaques ciblées passent beaucoup trop de temps à enquêter sur des événements, contribuant à un sentiment d'urgence, plutôt qu'à se concentrer pro-activement à la détection et à l'atténuation des menaces.
Le rapport met en évidence le fait qu'en France :
• Seulement 26 % des entreprises sont confiantes dans leur capacité à détecter une attaque en quelques minutes, et 29 % ont déclaré que cela pouvait leur prendre des jours, des semaines, voire des mois avant qu'elles ne remarquent un comportement suspect.
• 71 % des DSI interrogés ont indiqué que les attaques ciblées sont une préoccupation majeure pour leur entreprise.
• 54 % des entreprises ont enquêté sur plus de 10 attaques l'an dernier.
• 95 % de celles qui sont capables de détecter les attaques en quelques minutes possèdent une solution de gestion des évènements et des informations de sécurité (SIEM).
• Plus de la moitié des entreprises interrogées (61 %) ont indiqué qu'elles sont équipées des outils et des technologies nécessaires pour fournir une réponse rapide aux attaques. Cependant, les indicateurs critiques ne sont généralement pas isolés de la masse des alertes générées et provoquent une charge de travail supplémentaire aux équipes qui doivent passer au crible toutes les données des menaces.
« Pour garder la main sur les attaquants il faut relever le défi du temps dans la détection », déclare David Grout, Directeur Europe du Sud de McAfee, filiale d'Intel Security. « En simplifiant, grâce à une analyse intelligente et en temps réel, le travail frénétique de filtrage d'un large volume d'alertes et d'indicateurs d'attaques vous pourrez plus efficacement appréhender des événements pertinents et prendre des mesures pour contenir et détourner les attaques plus rapidement. »
Compte tenu de l'importance de l'identification des indicateurs critiques, le rapport de McAfee Intel Security a révélé le Top 8 des indicateurs d'attaque les plus courants.
Parmi ceux-ci, cinq reflètent le suivi des événements à travers le temps écoulé et montrent l'importance de la corrélation contextuelle :
1. Des hôtes internes communiquent vers des destinations inconnues ou mal connues ou vers un pays étranger où il n'y a pas d'affaire en cours.
2. Des hôtes internes communiquent vers des hôtes externes qui utilisent des ports non standards ou en inéquation avec le protocole/port, tels que l'envoi d'interpréteurs de commandes (SSH) plutôt que du trafic HTTP sur le port 80, qui est le port Web par défaut.
3. Des accès publiques ou en zone démilitarisée (DMZ) communiquant vers des hôtes internes. Cela permet de brûler les étapes de l'extérieur vers l'intérieur et en arrière-plan, permet l'exfiltration de données et l'accès à distance à des actifs. Il neutralise la valeur de la DMZ.
4. Détection de logiciels malveillants en heures Off. Ces alertes qui peuvent se produire en dehors des heures standards d'ouverture de l'entreprise (la nuit ou le week-end) et qui pourraient signaler un hôte compromis.
5. Scans de réseau par les hôtes internes communiquant avec plusieurs hôtes dans un court laps de temps, qui pourrait révéler une attaque se déplaçant latéralement au sein du réseau. Les défenses du périmètre réseau, tels que pare-feu et IPS, sont rarement configurées pour surveiller le trafic sur le réseau interne (mais pourrait l'être).
6. Plusieurs événements alarmants à partir d'un seul hôte ou à répétition sur une période de 24 heures sur plusieurs machines dans le même sous-réseau, tels que les échecs d'authentification.
7. Après avoir été nettoyé, un système est réinfecté par des logiciels malveillants dans les cinq minutes qui suivent – les réinfections répétées signalent la présence d'un rootkit ou d'une compromission persistante.
8. Un compte utilisateur tente de se connecter à de multiples ressources en quelques minutes à partir de ou vers différentes régions – signe que les informations d'identification de l'utilisateur ont été volées ou que l'utilisateur a des intentions suspectes.
« Un jour, nous avons remarqué qu'un poste de travail subissait des demandes d'authentification du contrôleur de domaine à deux heures du matin. Cela pouvait bien sur être tout à fait normal, mais il se pouvait aussi que cela soit un signe d'alerte malveillante », commente Lance Wright, directeur principal de l'information de sécurité et de conformité à Volusion, un fournisseur de solutions de commerce contributeur de l'élaboration du rapport. *« Suite à cet incident, nous avons créé une règle pour nous alerter si un poste de travail avait plus de cinq demandes d'authentification en dehors des heures ouvrables pour nous aider à identifier le début de l'attaque, avant que les données ne soient compromises. »*

« La veille en temps-réel, la bonne intelligence et les solutions de gestion des évènements et des informations de sécurité (SIEM), permettent de minimiser le temps de détection, d'éviter de manière proactive les violations fondées sur la contextualisation des indicateurs lors de l'analyse et d'apporter des réponses en matière d'action automatisés », précise David Grout *« Grâce aux solutions qui permettent d'accélérer la capacité de détection, de réaction et d'apprentissage sur les attaques, les entreprises peuvent grandement changer leur posture de sécurité et passer de 'traquées' à 'traqueuses'. »*

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.itrnews.com/articles/152073/chaque-minute-compte.html

---

Pour la première fois, les données d'un objet connecté sont utilisées en justice

Pour la première fois, les données d'un objet connecté sont utilisées en justice

Pour la première fois, les données récoltées par un #bracelet connecté sont exploitées dans une affaire judiciaire au Canada. Une démarche réalisée en même temps qu'un procès visant à déterminer les performances physiques d'une jeune femme blessée dans un accident. La première d'une longue lignée ?

Il y a 4 ans, une habitante de la ville de Calgary a été victime d'un accident de voiture qui aurait fortement diminué ses capacités physiques. De très sportive, la jeune femme est désormais limitée à des activités quotidiennes lambda : c'est la principale raison pour laquelle elle réclame aujourd'hui des dommages et intérêts. Et pour démontrer ses dires, ses avocats ont décidé de ne pas se baser uniquement sur une expertise médicale, mais également sur les données récoltées par un bracelet connecté Fitbit.

Une comparaison avec le reste de la population

L'étude des habitudes de la plaignante va durer plusieurs mois, pour avoir une base précise. Un bracelet de type Fitbit, appelé traqueur d'activité, mesure notamment le nombre de pas effectué au quotidien, les escaliers montés, ainsi que le sommeil. Les avocats ne comptent pas utiliser les données de manière brutes : elles seront traitées par Vivametrica, une entreprise spécialisée dans l'analyse d'informations récoltées par le biais d'appareils connectés. L'objectif est de positionner le comportement quotidien de la jeune femme vis-à-vis du reste de la population.

« Jusqu'à présent, nous nous basions uniquement sur l'interprétation clinique » explique l'avocat Simon Muller. « Désormais, nous cherchons à nous baser sur des périodes de temps plus longues qu'une seule journée, pour disposer de plus de données. » Au bout de plusieurs mois, l'avocat espère pouvoir démontrer que « le niveau d'activité de la victime a été revu à la baisse et compromis suite à sa blessure. » L'un des points bloquants de l'affaire se trouve dans le fait qu'il n'existe pas de données enregistrées avant l'accident : difficile, donc, de faire un avant et un après. Mais la démarche pose de tout de même question.

Le premier cas, mais pas le dernier ?

Si, dans le cas présent, la victime de l'accident se prête de bonne grâce à l'expérience, la situation pousse à réfléchir à l'usage des #objets connectés et des données liées dans le cadre d'affaires judiciaires. Selon Forbes, il s'agit de la première affaire en la matière, mais en cas de résultats concluants, la démarche pourrait se généraliser.

On peut notamment imaginer que, dans certains cas, par exemple liés à des litiges avec des assurances, ces dernières demandent à ce que des objets connectés soient utilisés pour fournir des preuves. Rick Hu, PDG de Vivametrica, explique que si les assurances ne peuvent pas elles-mêmes avoir de telles exigences, elles pourraient demander une ordonnance de tribunal pour récupérer des données stockées sur un service tiers. Une démarche qui, selon lui, n'est pas particulièrement différente de celle qui consiste à demander l'accès à des informations stockées sur Facebook, par exemple. D'ailleurs, le réseau social lui-même serait en train de plancher sur des applications en lien avec la santé : ce genre de réflexion n'est donc pas à négliger. (pour aller plus loin : Santé en ligne : Facebook veut-il jouer au docteur ?)

L'autre possibilité, c'est que l'utilisateur d'un dispositif de santé connecté fournisse sciemment l'accès aux données à un organisme d'assurance partenaire. L'exemple d'Apple HealthKit est intéressant sur ce point, puisque l'entreprise serait actuellement en discussion avec des organismes liés à la santé aux Etats-Unis, pour que ces derniers utilisent ses outils. Parmi eux, des compagnies d'assurances.

Des données au service de l'utilisateur… ou pas

Si les données récoltées par les appareils de mesure de soi permettent de se faire une idée sur ses habitudes et son état de santé et avoir un impact positif, elles peuvent également jouer en défaveur du porteur. Dans le cas d'une action en justice, la géolocalisation, les heures de sommeil et autres informations récupérées de manière automatique par un bracelet ou une montre connectée pourraient éventuellement confirmer ou réfuter les déclarations d'une personne.

Mais un tel procédé a également ses limites, car si les données sont évocatrices, il semble aujourd'hui difficile de démontrer qui portait vraiment l'appareil à un instant T. Une situation qui pourrait évoluer à l'avenir, avec le développement de systèmes biométriques plus performants, comme l'analyse de la sueur ou l'obligation d'utiliser une empreinte digitale pour activer un dispositif, par exemple. MasterCard teste depuis peu la reconnaissance du rythme cardiaque comme moyen de valider un paiement. De telles possibilités ne sont donc pas très éloignées de notre quotidien, de plus en plus lié à une collecte intensive de données personnelles.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.clubic.com/mag/sport/actualite-739717-canada-donnees-recoltees-bracelet-connecte-utilisees-proces.html?estat_svc=s%3D223023201608%26crmID%3D639453874_748427012
par Audrey Oeillet

Une députée propose que la famille puisse supprimer les

données d’un proche décédé

Identité numérique des défunts : Une députée propose que la famille puisse supprimer les données d’un proche décédé

La suppression des données personnelles présentes en ligne, même après le décès d’une personne, reste actuellement dans le flou. Une députée demande à ce que les proches puissent faire retirer ces informations.

Afin d’aider les familles à gérer la mort d’un proche, des procédures permettant de supprimer les comptes en ligne existent. Parfois complexes, elles autorisent toutefois à ce que des membres d’une même famille puissent empêcher que les informations soient utilisées ou que le compte subsiste.

Lorsqu’un tel événement survient, la personne qui se charge de cette tâche doit donc généralement passer par des formulaires en ligne, tous différents, en fonction du service ciblé. Une tâche qui peut donc s’avérer fastidieuse, lorsque plusieurs plateformes (ou ensemble tels que la constellation Gmail, YouTube, Drive…) sont pris en compte.

Face à cette complexité, la députée socialiste Edith Gueugneau demande à ce que les règles en la matière soient plus précises. Dans une question adressée à Axelle Lemaire, secrétaire d’Etat chargée du numérique, l’élue estime que la loi est à ce jour « imprécise sur le devenir de ces données après le décès de l’utilisateur » et considère qu’il est : « particulièrement difficile pour les proches du défunt d’obtenir l’effacement de ces données. La loi ne prévoit pas non plus de délai d’exécution de la demande ».
C’est pourquoi elle demande que la loi puisse donner aux proches d’une personne décédée un droit, afin qu’ils puissent faire effacer ces données personnelles. La députée PS souhaite pour cela associer FAI, moteurs de recherche ainsi que les services de l’état civil.

Si l’idée d’un effacement complet du Web ne paraît pas réaliste, certaines pistes pourraient conduire à cette finalité. La procédure de « droit à l’oubli » mise en place par les moteurs de recherche pouvant par exemple être étendue à cet effet. Toujours est-il qu’il revient désormais à Axelle Lemaire de se pencher sur cette question.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-739481-donnees-mort-flou.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_18/11/2014
par Olivier Robillart

Airbus Helicopters a-t-il été victime d’un piratage informatique américain?

Airbus Helicopters a-t-il été victime d'un piratage informatique américain?

Selon des sources concordantes, Airbus Helicopters a été victime d'une attaque informatique. Le constructeur a de « fortes suspicions » d'une attaque venant des États-Unis.

C'est peut-être une affaire d'État. Certes ce qui s'est passé chez Airbus Helicopters n'est pas réellement surprenant mais si l'enquête des autorités françaises en cours confirme les « fortes suspicions » du constructeur de Marignane, selon des sources concordantes, elle mettrait une nouvelle fois en lumière les pratiques détestables d'espionnage des États-Unis à l'égard de leurs alliés malgré toutes les conséquences néfastes sur le plan diplomatique de l'affaire Snowden. Ce qui est sûr, selon ces mêmes sources, c'est que Airbus Helicopters a bien été victime d'une attaque informatique, dont l'ampleur reste encore à déterminer.
Le constructeur de Marignane s'est récemment aperçu d'une intrusion ou d'une tentative d'intrusion dans ses réseaux de communications. Alerté par Airbus Helicopters, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'autorité nationale en matière de sécurité et de défense des systèmes d'information, a lancé une enquête pour savoir si les intrusions ont réussi et, si c'est le cas, pour déterminer l'ampleur des dommages. Contacté par La Tribune, Airbus Helicopters affirme qu' »aucune information classifiée » n'a été dérobée. Mais, selon des sources concordantes interrogées par La Tribune, le constructeur nourrit de « fortes suspicions » vis-à-vis des États-Unis. « Mais nous n'avons pas encore d'éléments pour le démontrer », explique-t-on chez le constructeur à La Tribune.

En jeu, un important appel d 'offre en Pologne
Pourquoi les États-Unis ? Selon ces mêmes sources, le constructeur suspecte s'être fait « piraté » dans le cadre de l'appel d'offres international lancé par la Pologne, qui veut acheter 70 hélicoptères de transport pour un montant estimé à 2,5 milliards d'euros environ. Les trois compétiteurs – l'italien AgustaWestland (AW149), Airbus Helicopters (Caracal ou EC725) et l'américain Sikorsky (S-70) attendent une décision de Varsovie fin 2014, voire début 2015. Les candidats ont jusqu'au 28 novembre pour déposer leurs offres. Jusqu'ici la compétition entre Airbus Helicopters et Sikorsky était très, très chaude.
Depuis plusieurs jours, Sikorsky joue d'ailleurs un drôle de jeu en Pologne. Les Américains veulent vendre des hélicoptères dont les performances ne correspondent pas au cahier de charge établi par Varsovie. Ce sont des appareils d'ancienne génération qu'ils ont en stock. Le ministère polonais de la Défense a répliqué fin octobre sur un ton extrêmement ferme à un courrier du président du consortium Sikorsky Aircraft Corporation (SAC) Mick Maurer, en affirmant que c'est à lui qu'appartient de « définir les besoins des forces armées et non au soumissionnaire de lui indiquer ce qu'il a à vendre ».

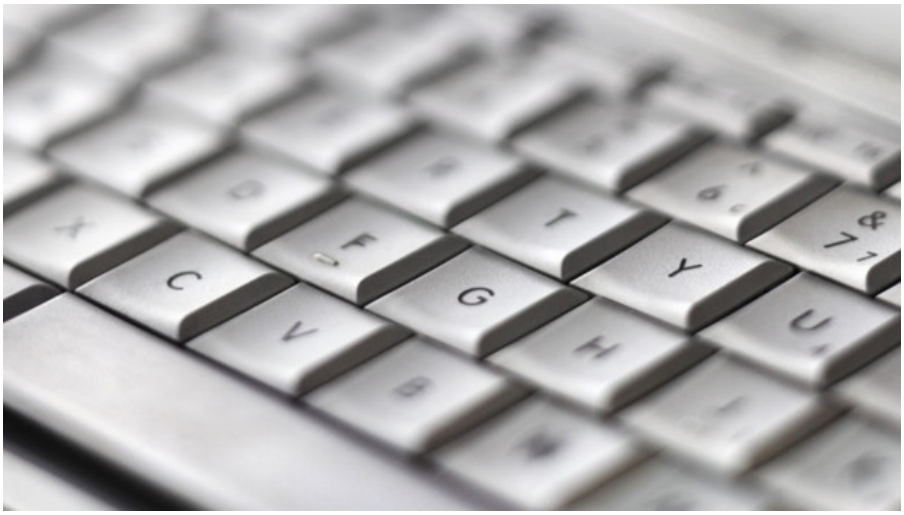
Que va faire Sikorsky ?
« Les exigences concernant l'hélicoptère multitâche étaient connues depuis mai dernier et la société SAC dispose d'appareils qui y répondent », a relevé le ministère polonais, avant de noter que « les autres candidats ont annoncé qu'ils présenteraient des offres correspondant aux exigences de l'Inspection de l'Armement ». Le ministère « ne prévoit pas d'annuler l'appel d'offres ou d'en modifier les termes au détriment de la Pologne », a assuré Varsovie, laissant entendre que tel était le sens de la lettre de Sikorsky. Il « reste ouvert à un dialogue équitable avec tous les candidats, mais ne cède pas aux pressions de contractants potentiels concernant les termes de la commande ».
Du coup, le 30 octobre, Sikorsky Aircraft a annoncé qu'elle ne participerait pas à l'appel d'offres pour la fourniture de 70 hélicoptères à la Pologne si les termes n'en sont pas modifiés. Le constructeur a précisé qu'il ne présenterait pas de proposition avec son partenaire polonais PZL Mielec car il lui semble impossible de livrer ses hélicoptères Black Hawk dans les conditions définies par l'appel d'offres. Dans un communiqué, le ministère polonais de la Défense a qualifié cette attitude de tactique de négociation, ce qu'a démenti Sikorsky. Le ministère a confirmé qu'il n'envisageait pas de modifier les termes de l'appel d'offres.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20141113trib0392bd0ed/airbus-helicopters-a-t-il-ete-victime-d-un-piratage-informatique-americain.html

---

Cyberattaque contre le département d'Etat américain



Cyberattaque contre le département d'Etat américain

Après des attaques contre le réseau informatique de la Maison Blanche le mois dernier et celui de la Poste américaine il y a quelques jours, ce serait désormais le département d'Etat américain qui aurait été victime de piratage.

Le département d'Etat américain a dû déconnecter ce week-end son réseau informatique non confidentiel après des soupçons de piratage, ont rapporté les médias américains. Vendredi, le département d'Etat avait invoqué une opération de maintenance de routine sur son principal réseau non confidentiel, affectant le trafic de courriels et l'accès aux sites internet publics.

Mais, selon des informations de presse publiées dimanche soir, un pirate informatique est soupçonné d'avoir franchi certaines barrières de sécurité du système gérant les courriels non classifiés. Selon un haut responsable cité par le Washington Post, une « activité inquiétante » a bien été constatée mais aucun des systèmes confidentiels n'a été touché.

Série de cyberattaques contre les organismes publics

Si elle se confirme, cette attaque informatique contre le département d'Etat serait la dernière d'une série de cyberattaques visant les organismes publics américains. La semaine dernière, la Poste américaine (USPS) avait annoncé que des pirates informatiques avaient volé des informations sur leurs employés et sans doute sur certains clients.

Jusqu'à environ 800.000 personnes rémunérées par la Poste américaine, y compris les sous-traitants, pourraient être concernées par ce piratage, selon un porte-parole de l'entreprise publique. Les pirates se seraient aussi introduits dans le système de paiement des bureaux de poste et en ligne, ce qui impliquerait aussi des clients, selon l'USPS. Le FBI a annoncé l'ouverture d'une enquête.

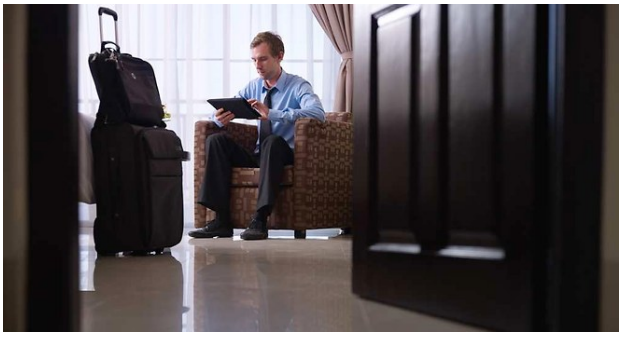
Le mois dernier, la Maison Blanche avait elle aussi fait état d'une « intrusion » dans son réseau informatique non confidentiel. Selon le Washington Post, des hackers russes sont soupçonnés d'en être à l'origine.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://lci.tf1.fr/monde/amerique/le-departement-d-etat-americain-victime-d-une-cyber-attaque-8519395.html

Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »



Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »

« Dark hotel » : ces hackers qui exploitent les réseaux Wi-fi des hôtels de luxe.
Des hackers ont pris pour cible des directeurs généraux et autres cadres dirigeants d’entreprises lorsqu’ils voyagent à l’étranger. Un phénomène qui durerait depuis quatre ans.
Nom de code « Dark Hotel ». Ce nouvel acteur dans le monde du cyberespionnage sévit depuis au moins quatre ans, révèle la société de sécurité russe Kaspersky Lab. **Ses cibles appartiennent à l’élite économique internationale : directeurs généraux, vice-présidents, directeurs des ventes et marketing de grosses entreprises américaines et asiatiques**. Pour les piéger et leur dérober des données sensibles, ces hackers mettent à profit les réseaux Wi-fi des hôtels de luxe dans lesquels ils voyagent.

Ces hackers sans visage ont un mot d’ordre : ne jamais frapper deux fois la même cible. Leur mode opératoire ? Un faux logiciel, de type Adore Reader ou Google Toolbar, que le visiteur est invité à télécharger après s’être connecté au réseau Wi-fi de son hôtel. Un cheval de Troie permet ensuite au hacker de recueillir des données privées, y compris les mots de passe sur Firefox, Chrome, Internet Explorer ainsi que les identifiants sur Gmail, Yahoo,Facebook et Twitter.

Les victimes se font ainsi voler des données qui relèvent du domaine de la propriété intellectuelle des entreprises qui les emploient. Après l’opération, toute trace est effacée du réseau de l’hôtel, le hacker retournant dans l’ombre. Une « précision chirurgicale », souligne Kaspersky Lab.

Selon l’unité de recherche de la société russe, une empreinte laissée par les hackers suggère que les cybercriminels parlent coréen. Le plus haut volume d’activité a été détecté entre août 2010 et 2013. 90 % des cyberattaques étaient localisées au Japon, Taïwan, en Chine, en Russie et en Corée du Sud. Depuis 2008, elles se comptent par milliers. Kaspersky Lab n’est, pour l’heure, pas parvenu à tracer ces hackers.

A partager sans modération

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lesechos.fr/tech-medias/hightech/0203938482430-dark-hotel-ces-hackers-qui-exploitent-les-reseaux-wi-fi-des-hotels-de-luxe-1064496.php
Aurélie Abadie

---

40 % des employés des grandes entreprises américaines

utilisent leurs matériels personnels, mais…

40 % des employés des grandes entreprises américaines utilisent leurs matériels personnels, mais…

Selon une récente étude réalisée par Gartner, le BYOD (Bring Your Own Device) serait appliqué par 40 % des employés des grandes entreprises aux États-Unis. Mais un point majeur est à préciser : les entreprises sont loin d'être toutes au courant d'un tel usage.

Le BYOD tiré par les employés, non les employeurs

Dans mes précédents papiers publiés ces derniers mois, je suis souvent revenu sur le risque numéro un de ne pas appliquer de politique de BYOD : que les employés utilisent dans le dos de l'entreprise leurs propres appareils, multipliant ainsi les risques de fuites et de sécurité.

Or dans sa dernière étude, si Gartner montre que 40 % des employés des grandes entreprises sont concernés par le BYOD, il faut bien comprendre que seule une partie minoritaire d'entre eux le font sur demande de la société. Plus précisément, nous apprenons qu'un quart des employés concernés le font suite à un besoin express de leur entreprise.

Cela signifie donc que les 75 % restants le font sans qu'il n'y ait de demande particulière. Or seule la moitié des entreprises sont au courant de ces agissements. L'autre moitié de ces 75 % ignore donc totalement ces utilisations. Non seulement cela prouve et confirme que le BYOD aux États-Unis est plus tiré par les employés que par les entreprises elles-mêmes, mais aussi et surtout qu'une partie importante d'entre elles prennent des risques importants du fait de leur manque de politique de BYOD.

La statistique est un claque terrible dès lors que cela signifie qu'environ 15 % des employés de toutes les grandes entreprises américaines apportent et utilisent leurs smartphones, leurs tablettes ou leurs PC portables dans le dos de leurs dirigeant. Une donnée catastrophique qui doit donner des sueurs froides à bien des DSI.

On se rappellera d'ailleurs qu'en mai dernier, ce même Gartner indiquait qu'un quart des employés américains utilisant leurs propres appareils avaient dû faire face à des problèmes de sécurité en 2013. Et une partie non négligeable d'entre eux (27 %) l'ont précisé à leur hiérarchie… Un cauchemar en puissance pour les entreprises concernées.

L'ignorance, la pire des situations

Toujours du côté des rappels, deux anciennes études ces derniers mois ont montré que de très nombreuses entreprises n'ont toujours aucune politique de BYOD et que bien peu appliquaient un « Full BYOD ». Si l'on cumule ces informations avec le fait que certains employés confondent BYOD et liberté totale, le résultat ne peut mener qu'à des catastrophes.

« La clé pour disposer d'un appareil sécurisé est de vous assurer qu'il est bien géré » notait fort justement Gartner il y a quelques mois. Or comme je l'ai maintes fois répété, manquer de clarté avec ses employés sur le sujet si épineux des appareils mobiles personnels est un danger gigantesque pour l'entreprise. S'il n'y a pas de politique de BYOD, il faut se montrer ferme. Si une politique est mise place, il ne faut pas semer de doute dans l'esprit des employés et leur préciser les meilleurs comportements à avoir.

Notons enfin qu'il est intéressant d'apprendre que les tablettes tactiles, que ce soit en entreprise ou à la maison, servent avant tout… à jouer. Le jeu passe ainsi juste devant les réseaux sociaux et la lecture d'actualité. « L'importance des jeux sur des tablettes va de paire avec la relativement faible utilisation des appareils à des fins de travail » résume Gartner, qui explique donc que globalement, les entreprises ont un besoin encore assez limité de ce type d'appareils, bien plus utilisé à la maison.

Par Nil Sanyas pour Bring it on

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/40-des-employes-des-grandes-entreprises-americaines-utilisent-leurs-materiels-personnels-mais-39809253.htm