Alerte : Une mise à jour Windows à supprimer d’urgence…

Alerte : Une mise à jour Windows à supprimer d’urgence…

Installée automatiquement pour la plupart des ordinateurs fonctionnant sous Windows 7, 8 et 8.1, la mise à jour de sécurité Microsoft Windows (KB2982791) est à supprimer de toute urgence.

Alerte à l’écran bleu, le fameux BSOD (Blue screen of death) ou ralentissements anormaux semblent être les principaux symptômes.
Microsoft a retiré le lien vers sa mise à jour de sécurité 2982791. L’éditeur dit avoir découvert trois problèmes à la suite de plantages d’utilisateurs. Le bulletin MS14-045 révisé vendredi dernier avertit de certains comportements liés à l’update.
Microsoft recherche les causes et préviendra dès qu’il en saura plus. En attendant, il recommande aux utilisateurs de **désinstaller la mise à jour 2982791**. Par précaution, il a lui-même enlevé la possibilité de la télécharger. Le bulletin MS14-045 concerne Windows 7, 8 et 8.1 ainsi que Windows Vista et Windows Server 2003.

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

Références :
http://www.lemondeinformatique.fr/actualites/lire-microsoft-retire-une-mise-a-jour-de-windows-qui-pose-probleme-58342.html

---

Enfin une protection contre les attaques informatiques de type DDoS ?

Enfin une protection contre les attaques informatiques de type DDoS ?

Comment lutter efficacement contre les attaque de type DDoS ? Telle est la problématique que Google souhaite résoudre en lançant son Project Shield tout en faisant appel aux sociétés souhaitant participer à ce programme.
Le DDoS (**D**istributed **D**enial **O**f **S**ervice) est l'une des attaques les plus fréquentes sur Internet. Celle-ci consiste à paramétrer plusieurs ordinateurs ou serveurs lançant des requêtes automatiques et répétées vers un serveur afin de le rendre inaccessible. Google explique que ce type d'opérations est relativement facile à mettre en place et peu coûteux.
DDoS
Pour prévenir les organisations n'ayant pas les moyens de parer ce type d'attaques, la firme de Mountain View lance alors le Project Shield (« bouclier » en français). Ce dernier repose sur le service Page Speed, initialement présenté sous la forme d'un module pour le serveur Apache en novembre 2010 puis proposé en tant que DNS pour rediriger le trafic vers les serveurs de Google. Il en résulterait un gain de performances aux alentours de 50%.
Avec Project Shield, le trafic des sites Internet passera donc via l'infrastructure de Google, et ceux-ci bénéficieront alors d'un même niveau de protection. Pour tester ce dispositif, le géant de la recherche propose aux sociétés intéressées de remplir un formulaire afin de recevoir une invitation. Google cherche tout d'abord des testeurs « de confiance », c'est-à-dire des agences de presse ou des organisations politiques ou impliquées dans le droit des hommes.
Ces participants seront invités à configurer Page Speed ainsi que leur domaine. **Pour l'heure le dispositif est gratuit mais Google n'exclut pas de le monétiser à l'avenir**.
Retrouvez davantage d'informations sur cette page
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.clubic.com/internet/google/actualite-594612-project-shield-google-souhaite-lutter-attaques-ddos.html

---

Droit à l'oubli – Quand on demande à Google d'oublier tout et n'importe quoi..

Droit à l'oubli – Quand on demande à Google d'oublier tout et n'importe quoi..

Google aurait reçu récemment une drôle de demande.
Selon le quotidien belge L'Avenir, Eden Hazard aurait rempli le formulaire de « droit à l'oubli » du moteur de recherches, afin que les (mauvaises) notes et les commentaires négatifs à son encontre ayant fait suite au quart de finale de la Coupe du monde entre la Belgique et l'Argentine (0-1) disparaissent.
Le joueur de Chelsea, cité notamment dans un article recensant les « 11 flops du Mondial », estimerait que ces critiques ternissent son image en vue d'une renégociation de contrat avec son club ou pour d'éventuels contrats publicitaires. **Google n'est en revanche pas obligé de valider cette demande**.

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

Références :
http://rmcsport.bfmtv.com/football/hazard-demande-a-google-d-effa-828188.html

---

Confidentialité des données : attention danger pour les DSI européens

Confidentialité des données : Attention danger pour les DSI européens

Les DSI ne peuvent se préoccuper des seuls aspects technologiques des projets conduits au sein de l'entreprise. Si les décideurs IT veulent et doivent peser plus dans les décisions business, ils doivent alors composer avec les risques liés à l'activité de l'entreprise et non seulement ceux ayant trait au système d'information.
C'est notamment le cas de la confidentialité des données client. Or, juge Forrester, il s'agit même désormais d'une priorité, en particulier pour les DSI européens en raison de la régulation dans ce domaine et de la préoccupation croissante des européens à l'égard de leurs données.
Vie privée : une préoccupation pour le client et l'entreprise
Et selon le cabinet, l'arrêt de la CUJE sur le droit à l'oubli rappelle aux DSI que la gestion des données personnelles s'impose comme une des grandes priorités business. « La régulation de la confidentialité est désormais un sujet que les DSI ne devraient pas sous-estimer en tant que risque majeur pour les entreprises ».
Car, prévient Forrester, **un incident impliquant des données client peut déboucher sur des conséquences plus que significatives, comme une sanction financière, un préjudice d'image pour l'entreprise et une perte de confiance de la part des consommateurs**.
Et pour le DSI lui-même, c'est son emploi même qui pourrait être en jeu. Victime d'un piratage informatique (vol des données bancaires de 40 millions de clients), l'enseigne américaine Target a poussé son DSI à la démission – suivie ensuite de celle du PDG.
Mais la confidentialité des données n'est-elle pas avant tout du ressort des métiers et notamment des services marketing et juridique ? Non, selon Forrester pour qui la DSI est directement impliquée dans la gestion de ces données.
Quid de la collecte et du stockage des données client
Les responsables des systèmes d'information interviennent ainsi dans le choix et le déploiement des solutions destinées à garantir la sécurité et l'intégrité de ces informations. Les DSI doivent également s'informer des mécanismes de collecte des données, de leur localisation et des usages associés (transfert, partage, etc.). En clair, connaître le cycle de vie de la donnée.
Et cela peut s'avérer complexe estime Forrester, par exemple lorsqu'un client de l'entreprise demande à exercer son droit à la suppression. « De nombreuses entreprises stockent les données client de façon redondante, par exemple pour chaque division ou chaque pays. De telles données peuvent aussi avoir été sauvegardées sur plusieurs serveurs, souvent à des localisations distinctes ».
« Ces structures complexes de stockage des données client transforment une suppression complète des données en un exercice difficile – certains disent impossible » commente l'analyste Dan Bieler. La problématique de la confidentialité des données comprend donc bien une dimension technologique et impose dès lors aux DSI de ne pas la négliger.
« Les entreprises qui conçoivent leur infrastructure IT en gardant à l'esprit la régulation de la confidentialité [Ndlr : privacy by design] disposent d'un avantage compétitif pour cet ère du client », en particulier dans un contexte d'accroissement du nombre de données collectées, de leur numérisation et de leur exploitation, par exemple dans le cadre d'un projet Big Data.

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

Références :
http://www.zdnet.fr/actualites/confidentialite-des-donnees-attention-danger-pour-les-dsi-europeens-39804963.htm

---

Et si le Cloud ne respectait pas vos données personnelles ?

Et si le Cloud ne respectait pas vos données personnelles ?

Seulement 1% des fournisseurs de Cloud est prêt pour la prochaine loi UE La grande majorité des fournisseurs de cloud ne sont pas encore préparés à répondre aux exigences de la nouvelle directive sur la protection des données, dite « EU General Data Protection Regulation », qui devrait entrer en application l'année prochaine. Une loi qui remplacera l'ancienne directive de 1995 sur la protection des données (EU Data Protection Directive).
Selon les conclusions d'une étude réalisée par le spécialiste de la sécurité de Skyhigh Networks, seulement 1 fournisseur de services cloud sur 100 est prêt pour respecter la nouvelle directive portant sur la protection des données. Une loi qui entend moderniser l'ancienne régulation pour s'aligner sur les contraintes imposées par Internet et le Cloud.
La nouvelle directive, qui devrait être votée en 2014 pour une implémentation en 2015, impose aux contrôleurs des données (les entreprises propriétaires des données), à ceux qui traitent les données (tels que les fournisseurs de cloud et les hébergeurs) de **partager leur responsabilité en matière de fuite de données et de violations de la loi**.
Cette nouvelle loi s'appliquera aux entreprises européennes qui traitent des données personnelles et aux entreprises hors de l'Europe, qui contrôlent les citoyens européens ou traitent des données personnelles obtenues à partir de biens ou de services offerts aux citoyens européens.
Un examen de plus de 7 000 services cloud, effectué par Skyhigh Networks , a ainsi révélé que les fournisseurs ont des problèmes évidents avec les contraintes imposées par la nouvelle loi, notamment au sujet de la résidence des données, de la détection et de la notification des fuites de données, du chiffrement et des politiques de suppression des données (le droit à l'oubli).
« Il est sidérant de constater que peu de fournisseurs cloud sont préparés aux nouvelles régulations européennes, mais heureusement, il reste encore du temps pour se mettre en conformité. Cela implique de résoudre dès maintenant un certain nombre de problèmes, comme le droit à l'oubli, et d'implémenter des politiques de protection des données qui soient conformes à ces nouveaux standards », affirme Charles Howe, directeur de Skyhigh Networks pour l'Europe.
Cette nouvelle loi vise également à renforcer la confiance des consommateurs et des entreprises dans l'économie numérique en Europe.
« Pour les fournisseurs de cloud, cela implique inévitablement des ressources ainsi que des dépenses supplémentaires, mais ce n'est rien comparé aux pénalités pour violation de la loi, qui peuvent atteindre jusqu'à 5% des revenus annuels d'une entreprises ou jusqu'à 100 millions d'euros. »
Ce qui tranche avec la directive de 1995 qui ne comportait aucune démarche en matière de pénalités. Ces lourdes amendes vont transformer la protection données en un enjeu crucial et obligeront les entreprises à passer en revue ce qu'elles doivent faire pour se mettre en conformité, soutiennent quelques experts.

Le droit à l'oubli – un parcours difficile
L'un des amendements les plus controversés est le droit à l'oubli – les individus ont le droit civique de demander que leurs informations personnelles soient supprimées d'Internet. « Il s'agit d'un problème complexe, mais étant donné l'intérêt des medias, il est peu probable que les fournisseurs de cloud soient pris par surprise », explique Howe.

« Un gros problème est que 63% des fournisseurs cloud conservent leurs données indéfiniment et n'ont aucune disposition en matière de rétention des données dans leurs conditions de vente », ajoute-t-il.

Une autre donnée vient s'ajouter : **23% des fournisseurs cloud gardent la notion de droit de partager les données avec d'autres entreprises tierces dans leur condition de vente**. Ce qui complique un peu plus le fait de garantir la suppression de toutes les données, a également révélé l'étude. « Il est juste de dire que le droit à l'oubli peut s'avérer être un vrai parcours du combattant pour de nombreuses entreprises – les fournisseurs de cloud eux-mêmes et leurs clients. Il ne s'agit pas que d'un problème pour Google », soutient Howe.

L'étude rapporte également que seulement 11 pays sont conformes aux contraintes de l'UE en matière de résidence des données. La loi impose que les entreprises ne stockent ni ne transfèrent des données dans des pays hors de la zone européenne qui n'ont pas de standards équivalents en matière de protection des données.

La question de la résidence des données se pose également pour fournisseurs de cloud avec des datacenters dans le monde, qui dans leurs opérations courantes peuvent transférer ou stocker des données dans des pays qui ne sont pas conformes aux règles européennes. Les Etats-Unis, où 67% des datacenters pour le cloud sont localisés, font partie de ces 11 pays.

La résidence des données sera une difficulté clé pour les services cloud lorsque la nouvelle loi entrera en vigueur – puisque seulement 8,9% des fournisseurs américains disposent de la Safe Harbour Certification, qui les exempte de cette contrainte, soutient Skyhigh Networks.

« Un brouillon de **la nouvelle loi obligeait les entreprises à notifier aux autorités européennes dans les 24 heures, une fuite de données**, même si celle-ci est intervenue dans un service cloud tiers. Le problème tient au fait que de nombreux fournisseurs de cloud tiennent expressément responsable le client de la détection de faille et cela peut être une opération impossible », ajoute encore Howe.

« Certaines régulations en place, comme au Royaume-Uni ou en France, permettent aux entreprises de contourner les contraintes liées à la notification de failles, si les données sont rendues inaccessibles via le chiffrement. Malheureusement, seulement 1,2% des fournisseurs de cloud propose la gestion des clés de chiffrement nécessaires pour cela », commente-t-il.

« La difficulté est que seuls quelques fournisseurs de cloud proposent des outils pour protéger nativement les données. En fait, seulement 2,9% des services cloud ont en place un système de mots de passe sécurisés. « La General Data Protection Regulation n'entre pas en application avant 2015, mais il reste encore beaucoup de travail à accomplir jusque-là », conclut Howe.

Lien pour télécharger l'étude :
http://info.skyhighnetworks.com/Cloud-Adopt–Risk-Report-July-2014_Registration.html

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

Références :
http://www.lemagit.fr/actualites/2240226789/Protection-des-donnees-1-fournisseur-de-cloud-sur-100-pas-pret-pour-la-prochaine-loi-UE

La CNIL lancera des contrôles à partir du mois d’octobre sur la gestion des cookies

	La CNIL lancera des contrôles à partir du mois d’octobre sur la gestion des cookies

La Commission Nationale de l'Informatique et des Libertés (CNIL) vient d'annoncer qu'elle allait mettre prochainement en oeuvre des contrôles sur internet pour vérifier l'application de la nouvelle législation relative aux cookies. Il est grand temps de mettre votre site internet en conformité !

La législation française relative aux cookies informatiques a été modifiée par l'ordonnance du 24 août 2011, qui a révisé l'article 32 II de la loi Informatique & Libertés du 6 janvier 1978.
Depuis lors, l'utilisation de ces cookies est soumise à l'information préalable des internautes, voire également à leur consentement préalable si le cookie n'a pas une finalité purement technique (comme ceux utilisés pour mémoriser un panier d'achat sur un site commerçant, par exemple).
D'une part, la loi énonce le principe selon lequel l'utilisateur doit être informé « de manière claire et complète » de tout traitement de ses données à caractère personnel.
Ceci suppose que l'utilisateur ait pu prendre connaissance, avant la pose du cookie, de l'objet de ce cookie (ce dont il s'agit) et de sa finalité (ce à quoi il vise), ainsi que de la possibilité de s'opposer à cette pose.

Avant la modification de la loi en France, cette information préalable prenait parfois la forme d'une simple clause dans les Conditions générales de vente ou les Conditions générales d'utilisation des sites internet utilisateurs de cookies.
Désormais, la CNIL considère qu'une telle clause n'est pas suffisante. Si elle reste possible, elle doit être assortie d'une mention plus explicite, par exemple sous la forme d'un bandeau diffusé sur la page d'accueil du site.
D'autre part, en ce qui concerne l'obtention du consentement des internautes, la loi dispose que « l'abonné ou la personne utilisatrice [doit avoir] exprimé, après avoir reçu cette information, son accord ».
Après consultation des acteurs et notamment des annonceurs professionnels, la CNIL considère désormais que, si le consentement doit toujours se manifester par le biais d'une « action positive » de la personne préalablement informée des conséquences de son choix et disposant des moyens de l'exercer, ce consentement peut être simplement présumé si l'internaute a été explicitement informé que la poursuite de la navigation vaut accord du dépôt du cookie.
Le consentement de l'internaute peut donc être présumé, sous réserve que l'information préalable ait été suffisamment claire et explicite. Mais en tout état de cause, l'internaute doit toujours pouvoir revenir sur son consentement et s'opposer ultérieurement à l'utilisation des cookies par un site internet. En d'autres termes, il est fondamental que tout site internet prévoie une page dédiée spécifiquement aux cookies, indiquant leur finalité et mettant en place un système d'opposition.
A ce jour, si l'on constate que de nombreux sites internet se sont conformés à la nouvelle législation, tous n'ont pas encore été modifiés : parfois, non seulement les internautes ne sont pas informés de l'utilisation de cookies par le biais d'un bandeau sur la page d'accueil du site, mais leur consentement n'est pas recueilli. De même, certaines conditions générales d'utilisation se contentent de préciser que le site utilise des cookies, sans faire la moindre référence à la notion de consentement.
Or la CNIL vient d'annoncer qu'elle allait contrôler le respect de la nouvelle règlementation à partir du mois d'octobre 2014. Si elle a laissé le temps aux opérateurs de se conformer aux nouvelles dispositions légales, le temps de la transition est terminé. La CNIL va utiliser ses pouvoirs de vérification sur place ainsi que ses nouveaux pouvoirs de contrôle en ligne.
La CNIL annonce qu'elle contrôlera le type de cookies utilisé, leur finalité, ainsi que les modalités de recueil du consentement, la visibilité, la qualité et la simplicité de l'information relative aux cookies.
L'autorité indique que, selon le bilan des contrôles qu'elle sera conduite à effectuer, elle pourra adopter des mises en demeure voire des sanctions à l'égard des entités qui n'auront pas respecté la loi.
Il est donc urgent, pour chacun des exploitants de site internet, de se mettre en conformité avec cette nouvelle législation.

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

Références :
http://www.journaldunet.com/ebusiness/expert/58185/cookies–la-cnil-lancera-ses-controles-a-partir-du-mois-d-octobre.shtml

---

Augmenter la sécurité des transactions sur Internet, le

défi de la nouvelle technologie IST Model

	**Augmenter la sécurité des transactions sur Internet, le défi de la nouvelle technologie IST Model**

IST Model (Intrinsic Security Technology Model) est une technologie qui permet d'augmenter considérablement la sécurité des transactions électroniques sur internet. Née comme une puissante méthode d'identification des utilisateurs sur des réseaux non protégés, elle a été spécialement conçue pour être robuste à de nombreuses attaques informatiques telles que le phishing, pharming, arp poisoning, etc.
Cette technologie, déjà brevetée en Italie, vient d'achever avec succès le processus d'enregistrement du brevet de l'US Patent Office, le Bureau de Brevets des Etats-Unis.

En utilisant une approche différente et complémentaire par rapport au chiffrement, IST Model garantit une sécurité intrinsèque au cours d'une transaction électronique entre deux ou plusieurs partenaires, quelle que soit la tâche, et pour toute sa durée. Conçu comme un protocole ouvert, IST Model peut être implémenté sur tous les standards et protocoles de communication existants. Le moteur interne de cette technologie assure des algorithmes rapides, pouvant être mis en oeuvre même sur de petits dispositifs.
Un premier champ d'application possible pour cette technologie est le domaine du commerce électronique sur internet, mais de manière plus générale, il est possible d'utiliser IST Model dans tous les domaines d'activité où il est nécessaire d'identifier les partenaires d'une transaction électronique, par exemple pour un nouveau passeport électronique, un système électronique d'ouverture/fermeture de portes/voitures/coffre-fort, un vaisseau spatial qui reçoit des commandes du centre de contrôle sur Terre etc.
L'utilisation idéale de cette technologie est le smartphone en réseau, mais tout appareil électronique peut en être équipé.

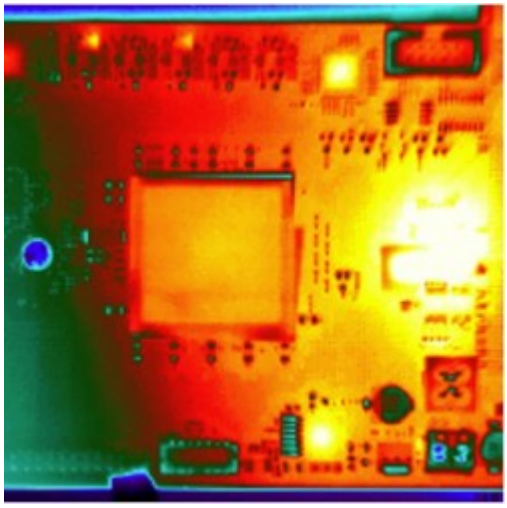
Source :
http://newsspazio.blogspot.it/2014/03/un-nuovo-brevetto-usa-per-uninvenzione.html

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

Références :
http://www.bulletins-electroniques.com/actualites/76521.htm

IBM invente le futur cerveau de nos futurs objets

connectés. Un pas de plus vers le robot humain ?



IBM invente le futur cerveau de nos futurs objets connectés. Un pas de plus vers le robot humain ?

La puce TrueNorth d'IBM pourrait peupler l'Internet des objets

Quand elle sera au point, la puce TrueNorth pourrait faire office de capteur basse consommation pour les appareils embarqués et portables.

IBM a franchi une nouvelle étape dans son ambitieux projet de processeur fonctionnant comme un cerveau humain. Big Blue a mis au point une seconde **puce, plus évoluée, qui imite la façon dont fonctionne le cerveau des mammifères**. « C'est une avancée supplémentaire vers les ordinateurs synaptiques », a déclaré Dharmendra Modha, Chief scientist au sein d'IBM Research, spécialisé en informatique synaptique. Des chercheurs de Cornell Tech ont aussi contribué à l'élaboration de la puce. Dans la revue Science de cette semaine qui consacre un article au prototype, Dharmendra Modha déclare que « l'architecture de TrueNorth tend à reproduire la structure et le fonctionnement du cerveau humain au niveau du silicium, tout en étant efficace sur le plan énergétique ». Quand elle sera définitivement au point, cette puce pourrait faire office de capteur basse consommation pour les appareils embarqués et portables. « TrueNorth pourrait devenir le cerveau en silicium de l'internet des Objets et transformer totalement notre expérience mobile », a encore déclaré le directeur scientifique.

La puce pourra également être intégrée dans les superordinateurs pour augmenter leur capacité d'apprentissage automatique et prendre en charge d'autres calculs capables de fonctionner avec les réseaux neuronaux. En 2011, l'équipe d'IBM dirigée par Dharmendra Modha avait déjà sorti une puce imitant le cerveau. Cette seconde puce «TrueNorth » compte 5,4 milliards de transistors entrelacés dans un réseau sur puce de 4096 noyaux neuro-synaptiques. Cela représente l'équivalent de 256 millions de synapses, soit beaucoup plus que la version 2011 qui en comptait 260 000 environ.

Facilement adapté à de grandes mises en oeuvre

IBM a également associé 16 puces « TrueNorth » entre elles par groupe de quatre fois quatre qui offrent collectivement l'équivalent de 16 millions de neurones et de 4 milliards de synapses. L'expérience vise à montrer que le prototype peut être facilement adapté à de grandes mises en oeuvre. Ce projet de puce intelligente avait été lancé en 2008 par le Defense Advanced Research Projects Agency (DARPA) américain sous le nom de Systems of Neuromorphic Adaptive Plastic Scalable Electronics (SyNAPSE). Ces nouvelles puces rompent radicalement avec l'architecture informatique actuelle imaginée par von Neumann, où le traitement des calculs se fait en série. La nouvelle architecture se rapproche du fonctionnement du cerveau humain, dans le sens où chaque « noyau neurosynaptique » possède sa propre mémoire (« les synapses »), son processeur (« le neurone ») et son réseau de communication (« les axones »), et tous travaillent ensemble selon un mode opératoire orienté événement.

Le travail commun de ces noyaux pourrait permettre la reconnaissance des formes et d'autres fonctions de détection, comme dans le cerveau humain. Et de la même manière, la puce d'IBM a besoin de très peu d'énergie pour fonctionner : 70mW en moyenne, soit bien en deçà de ce que consommeraient les processeurs standards pour exécuter les mêmes opérations. Samsung a fabriqué la puce prototype en utilisant un procédé de gravure à 28 nanomètres. Le fait que « TrueNorth » consomme aussi peu d'énergie – moins qu'un appareil auditif – ouvre un vaste champ d'utilisations potentielles, en particulier sur les appareils disposant de ressources énergétiques limitées. Il serait par exemple possible d'intégrer ce processeur à un appareil mobile ou à un capteur, où il pourrait apprendre à reconnaître des objets après avoir analysé des sons, des images ou des sources multi sensorielles. Actuellement, il faudrait recourir au calcul intensif avec serveur dédié pour réaliser ce type d'analyses. Avec la puce, on pourrait facilement effectuer ces tâches sur un périphérique distant, sans avoir besoin de faire remonter les informations vers un centre de calcul. « Le capteur devient l'ordinateur », a déclaré Dharmendra Modha.

Prendre en charge l'apprentissage machine

L'architecture synaptique n'est pas destinée à remplacer les processeurs actuels, mais les deux types de puces pourraient être associées pour réaliser des tâches nécessitant beaucoup de puissance de calcul en parallèle. « Dans le datacenter, les puces pourraient être utilisées dans les cartes d'accélération pour coprocesseur pour faire tourner les réseaux neuronaux qui prennent en charge l'apprentissage machine », a expliqué Dharmendra Modha. « De nombreux algorithmes d'apprentissage machine utilisés actuellement peuvent être facilement adaptés à cette architecture. On pourrait effectuer des opérations de traitement hautement parallèles de façon plus efficace sur le plan énergétique », a-t-il encore déclaré.

IBM continue à explorer différentes applications possible pour son processeur, mais pour l'instant le constructeur ne s'est ni engagé à fabriquer la puce lui-même, ni à en vendre le design sous licence à d'autres fabricants. Dharmendra Modha a aussi précisé que dans le procédé de fabrication, son équipe n'avait n'a pas identifié d'obstacle particulier pour la production en masse. IBM est également en train de développer des compilateurs et des logiciels destinés à faciliter l'usage de ces processeurs.

Article de Jean Elyan avec IDG News Service

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

Références :

http://www.lemondeinformatique.fr/actualites/lire-la-puce-truenorth-d-ibm-pourrait-peupler-l-internet-des-objets-58299.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Attaque informatique contre les fournisseurs d’énergie – Dragonfly lance la cyberguerre froide…

Attaque informatique contre les fournisseurs d’énergie – Dragonfly lance la cyberguerre froide…
Le scénario du pire. Ou presque. Un groupe de hackers, baptisé Dragonfly, est parvenu à corrompre certains systèmes de contrôle des opérateurs d’énergie. Notamment en France. Les pirates avaient alors la possibilité de saboter la distribution d’énergie de certains pays.

Une victime des pirates informatique guidée en ligne pour payer la rançon

Une victime des pirates informatique guidée en ligne pour payer la rançon

Témoignage d'un client :
L'informaticien Robert Hyppolite a dû payer une rançon aux pirates de SynoLocker… qui lui ont offert une assistance en ligne.

«Imaginez une entreprise de conseil juridique qui perd tous ses documents: mémoires, pièces, scans.
C'est un énorme coup dur. Sans les pièces, il y a de quoi perdre un procès!» Robert Hyppolite travaille depuis trente ans dans l'informatique à Genève. Il a notamment fondé l'entreprise Infologo, rachetée par VTX. Depuis 2007, il propose à ses clients le produit Synology, un système d'exploitation pour les serveurs de stockage en réseau. Des pirates ont élaboré un virus baptisé «SynoLocker TM» (sic) qui exploite la faille de sécurité de certaines anciennes versions du système. La police genevoise prend connaissance de cinq à dix nouveaux cas chaque semaine. Sur les trente clients de Robert Hyppolite équipés de Synology, deux ont été infectés et leurs sauvegardes ont également été atteintes. L'informaticien a dû payer une rançon en urgence dans la nuit de mardi à mercredi: l'un des deux clients touchés demandait une solution immédiate.

«La première difficulté était qu'il fallait payer en bitcoins, explique-il. On ne peut pas en acheter du jour au lendemain: il faut ouvrir un compte, donner son identité, faire un virement… Pour gagner du temps, je suis allé au distributeur de bitcoins des Pâquis (lire: Le bitcoin gagne l'économie réelle à Genève). La somme exigée par les pirates est de 0,6 bitcoin, ce qui correspondait à 650 francs, mais le cours est très fluctuant et dépend des pays et des plates-formes. »

Contre paiement de la rançon, un code permet normalement de décrypter les données et de retrouver ses fichiers. Sauf que l'aventure ne s'est pas arrêtée là. «Le virus chiffre les fichiers avec une clé réputée inviolable (2048 bits), ce qui les rend inutilisable. Ils restent normalement visibles avec leur nom correct. Mais le système de cette entreprise n'a pas réagi comme les autres et a été entièrement corrompu.» Conséquence: il a fallu réinstaller le système d'exploitation Synology, puis… réinstaller le virus, pour pouvoir permettre le décryptage des fichiers au moyen du code.

Les pirates répondent en ligne
Comment installer soi-même un virus? L'informaticien fait une curieuse découverte: «Sur le site Internet des ravisseurs, on trouve un onglet «support»… avec un chat en direct. Ils m'ont répondu très poliment: «Cher Monsieur, nous avons pris note de votre problème…» J'avais l'impression de parler à l'assistance en ligne d'une compagnie officielle! Une heure après, ils m'envoyaient une marche à suivre: il fallait entrer manuellement des instructions en ligne de commande. Tout a fonctionné sauf la dernière opération. A nouveau, le support informatique des pirates m'a répondu: leur dernière instruction contenait une erreur. J'ai ensuite pu entrer le code et tout est revenu à la normale.»
Une sauvegarde sur un serveur ou un disque dur séparé aurait permis de récupérer les données sans être rançonné. «Je préconise toujours cette mesure, mais dès qu'il faut s'équiper, il n'y a plus personne, regrette l'informaticien. Les clients pensent qu'on veut leur vendre des produits ou services inutiles, sauf ceux qui ont déjà vécu un sinistre…»
L'entreprise Synology souffrira-t-elle du virus SynoLocker? «Oui, mais ce sera vite oublié, estime Robert Hyppolite. J'ai vécu la mise à jour de l'antivirus Avast qui rendait les machines inutilisables… Pendant une année, leurs ventes ont baissé. Depuis, ils se sont rattrapés.» L'informaticien devra encore résoudre le problème du second client pris en otage. L'occasion, peut-être, d'une nouvelle discussion avec des ravisseurs informatiques très organisés et qui semblent prendre soin de leurs «clients».
Note: en cas d'infection avec SynoLocker, la police recommande de ne pas s'acquitter de la rançon et de réinitialiser les disques durs. Dans une note publiée ce jeudi, la Confédération émet des recommandations contre SynoLocker et conseille un outil de décryptage gratuit contre un virus au fonctionnement semblable, Cryptolocker.
Lire la suite…
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.tdg.ch/high-tech/hard-software/Des-pirates-informatiques-guident-leurs-victimes-en-ligne/story/19256356