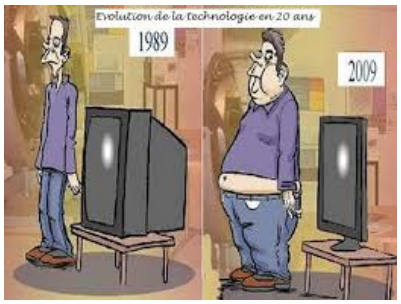
L’évolution des technologies inquiète…

	L’évolution des technologies inquiète…

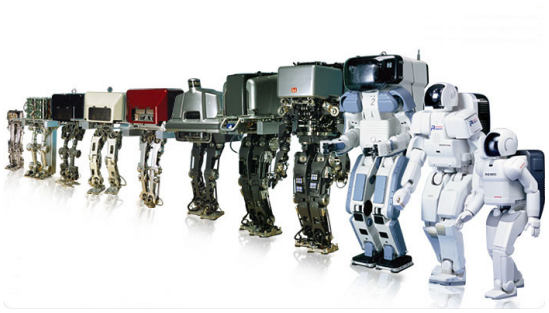
56% des répondants à l'enquête mondiale Global Evolving Worforce menée par TNS pensent que la technologie évolue trop rapidement et qu'elle aura un impact négatif sur eux. Ils s'attendent à une automatisation des tâches et craignent que le big data n'entrave leur liberté individuelle.

Si les utilisateurs sont persuadés que leurs smartphones, tablettes, PC portables et autres équipements informatiques les rendent plus productifs au bureau, ils s'inquiètent du rôle croissant de la technologie dans leur vie privée. Selon les résultats de l'étude Global Evolving Worforce menée auprès de 4764 employés dans une dizaine de pays, dont la France, 56% des sondés pensent en effet que la technologie a un effet néfaste sur eux. Les auteurs de ce rapport réalisé par le cabinet TNS pour le compte d'Intel et de Dell entre le 11 juillet et le 5 septembre dernier, ont indiqué que ces « downsiders » de la technologie estimaient que sa prolifération contribuait à la fois à les séparer et à les rendre moins importants. Ils pensent également que la technologie évolue trop rapidement et qu'ils ne peuvent plus suivre. Outre des doutes sur la responsabilité des entreprises à l'égard de leurs données personnelles, ils craignent que la tendance des big data se traduise par la fin de leur liberté individuelle.

Toutefois, certains s'attendent à ce que les big data soient utilisées à des fins de promotions internes ou d'évolution de carrière, De leur côté, près de 40% pensent que les recrutements seront effectués par des logiciels entièrement automatisés, plutôt que par des humains. Certains redoutent également d'être surveillés par des webcams lorsqu'ils travaillent chez eux. L'étude précise que les « downsiders » constituent la majorité des personnes interrogées dans des pays développés comme les États-Unis, Royaume-Uni, le Japon et la France, pays où la technologie est fortement implantée dans les entreprises. A l'opposé, les «upsiders »seraient majoritaires dans les pays émergents, comme la Chine, l'Inde et les Émirats arabes unis, l'IT faisant partie des habitudes de vie depuis moins longtemps.

Des évolutions graduelles plutôt que des bouleversements

Les upsiders (44% du total mondial) estiment pour leur part que la plupart des problèmes peuvent être résolus grâce à la technologie, et que celle-ci contribue à les rassembler. Pour eux, l'IT est un facteur clé qui améliore leur existence et sans elle, ils ne seraient pas heureux. Les auteurs du rapport pensent qu'avec le temps, on pourra déterminer qui des deux groupes a raison mais ils s'attendent à ce que la réponse soit à la fois valable pour l'un et l'autre ».Si l'on se penche sur les résultats obtenus par pays, 66% des répondants basés aux Etats-Unis considèrent que la technologie finira par atteindre une limite dans sa capacité à améliorer leur productivité, mais que cela n'arrivera pas tout de suite. Un peu moins d'un quart pensent que leurs emplois seront entièrement automatisés, tandis que sept sur dix jugent qu'il est préférable de faire réaliser certaines tâches par des humains En Chine, ils ne sont que 46% à penser la même chose.



En clair, ces actifs sont convaincus des gains de productivité résultant de la technologie et ils pressentent des changements graduels plutôt que des perturbations. 87% pensent que les tablettes remplaceront les PC (même si aucune date n'a été avancée), tandis que 92% estiment que la reconnaissance vocale finira par se substituer au clavier. «Je considère que ces personnes sont l'épine dorsale du travail réalisé et qu'ils vont incroyablement gagner en importance aujourd'hui et à l'avenir», a déclaré Steve Lalla, vice-président et responsable du cloud chez Dell. « Ce qui se passe, c'est que les collaborateurs souhaitent se rapprocher des clients », a-t-il ajouté. « Pour cela, ils doivent être mobiles et aller par monts et par vaux. La technologie permet de faciliter les choses, mais elle ne peut pas nécessairement tout faire. »

Une perception du télétravail qui diverge selon les pays

L'enquête Evolving Workforce menée par TNS a également dressé un état des lieux des tendances en matière d'habitudes de travail. 52% des répondants jugent que ceux qui sont habitués à travailler chez eux sont au moins autant productifs que s'ils travaillaient au bureau, 29% n'ayant pas d'opinion tranchée. Aux Etats-Unis, 40% jugent la productivité à domicile supérieure à celle au bureau, tandis qu'en Chine, cette part s'élève à 50%. Chez Dell, 20% des 100 000 collaborateurs du groupe font partie d'un programme de travail flexible, une proportion qui devrait atteindre 50% en 2020, La compagnie estime que cette pratique améliore la productivité de ses équipes.

Dans ses enquêtes internes, le groupe a constaté une augmentation de la satisfaction de ses salariés due à la mise en place du télétravail. De plus, la collaboration à distance lui aurait permis d'économiser 12 M$ et d'éviter 6 700 tonnes d'émissions de gaz à effet de serre.

L'enquête note en parallèle un écart important entre les pays sur les attitudes des entreprises envers le télétravail. Ainsi, l'Allemagne et le Japon ont une culture traditionnellement ancrée sur le travail réalisé au sein de l'entreprise. En France et en Allemagne, certains employeurs ont décidé de désactiver leurs plates-forme de messagerie durant les week-ends pour réduire la charge de travail de leurs employés. Dans le même temps, certains collaborateurs sont mieux équipés chez eux qu'au bureau et ont des accès plus rapides à Internet, « De ce fait, la pratique du travail est plus répandue qu'auparavant », a conclu Bob O'Donnell, fondateur de Technalysis Research.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-les-salaries-des-pays-developpes-inquiets-face-aux-nouvelles-technologies-59598.html
Article de Véronique Arène avec IDG NS
Personnalisation : Denis JACOPINI

Système d’appel d’urgence (eCall) obligatoire à partir d’octobre 2015

Système d’appel d’urgence (eCall) obligatoire à partir d’octobre 2015

A partir d’octobre 2015, tous les nouveaux véhicules vendus dans l’Union européenne seront équipés d’un service permettant de composer un numéro d’urgence en cas d’accident grave: le système eCall. C’est ce que prévoient les nouvelles règles qui seront votées par la commission du marché intérieur le 11 février 2014.

« eCall »: c’est le nom de ce système qui devrait sauver de nombreuses vies. En cas d’accident, le système eCall compose automatiquement le 112, et ce dès que ses capteurs (situés par exemple sur les airbags) enregistrent un choc. Le numéro pourrait également être activé manuellement, grâce à un bouton spécial. Le système est censé transmettre ensuite le lieu et l’heure de l’accident au centre de secours le plus proche.

« Le système eCall pourrait sauver jusqu’à 2500 vies par an, ce qui est selon moi un argument décisif pour l’introduction de ce service public d’appel d’urgence dans toute l’Union européenne », a déclaré le rappoteur Olga Sehnalová, députée démocrate socialiste tchèque.

D’ici là, les Etats membres devront améliorer leur infrastructure de manière à ce que les eCalls aboutissement directement aux services d’urgence.

Aujourd’hui, seuls 0,7 % de tous les passagers dans l’Union européenne sont équipés de systèmes automatiques d’appels d’urgence. Le coût d’une installation de l’outil eCall est estimé à moins de 100 euros par véhicule.

Voir aussi sur le même sujet « Installation obligatoire d’eCall dans les véhicules à partir de 2015 »
http://www.techno-science.net/?onglet=news&news=11767

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.techno-science.net/?onglet=news&news=12481

2015 sous haute tension en matière de Cybercriminalité

	2015 sous haute tension en matière de Cybercriminalité

Les cybercriminels sont de plus en plus confiants : ils avaient auparavant tendance à attaquer les usagers de services bancaires, voyant en eux le maillon faible de la chaîne de sécurité, mais les experts de Kaspersky Lab anticipent désormais des cyber-attaques ciblées d'envergure sur les banques elles-mêmes. Et les fraudeurs ne s'arrêteront pas là!

Ils devraient tenter le tout pour le tout en essayant de développer de nouveaux malwares capables de retirer du liquide directement depuis les distributeurs. Outre les cyber-crimes financiers, 2015 suscitera probablement encore plus d'inquiétudes quant à la confidentialité et à la sécurité des appareils Apple, et fera resurgir les peurs quant aux appareils connectés ; il s'agira d'empêcher les hackers d'utiliser des outils comme les imprimantes réseau pour pénétrer les réseaux d'entreprises.

1. Quand les cybercriminels s'inspirent des APT
Lors d'une étude récente, nous avons découvert une attaque dans laquelle l'ordinateur d'un comptable a été compromis et utilisé pour effectuer un transfert important avec une institution financière. Cela illustre une tendance intéressante : celle des attaques ciblées contre les banques elles-mêmes.
Nous assistons à une augmentation des incidents provoqués par des malwares dans lesquels les banques sont infiltrées en utilisant des méthodes utilisées dans les APT. Une fois que les pirates ont pénétré les réseaux de la banque, ils volent assez d'informations pour pouvoir voler de l'argent directement à la banque et ce, de plusieurs manières :
• En prenant le contrôle des distributeurs automatiques à distance afin d'obtenir du liquide
• En réalisant des transferts SWIFT depuis plusieurs comptes de clients
• En manipulant les systèmes bancaires en ligne pour réaliser des transferts en arrière-plan
De telles attaques annoncent l'émergence d'une nouvelle tendance qui s'inspire des attaques APT que l'on voit dans le monde cybercriminel.

2. Les groupes se fragmentent, les attaques APT se diversifient
La révélation de l'existence de ces groupes utilisant les APT a mené à l'exposition publique et la condamnation d'un groupe de pirates qui aurait mené des actions de cyber-espionnage contre des entreprises américaines.
Alors que les équipes de recherche continuent d'encourager la découverte de ces groupes ayant recours aux APT, nous nous attendons à des changements en 2015 : les groupes d'APT les plus importants et les plus connus se sépareront en plus petits groupes qui fonctionneront indépendamment les uns des autres. Les attaques deviendront plus répandues et davantage d'entreprises seront touchées car les petits groupes diversifieront leurs attaques. Cela signifie également que les entreprises les plus importantes qui ont déjà été compromises dans le passé par deux ou trois groupes d'APT importants (comme par exemple, 'Comment Crew' et 'Webky') seront la cible d'attaques plus diverses et provenant de plusieurs sources différentes.

3. Un ancien code, de nouvelles vulnérabilités (dangereuses)
De récentes accusations d'altération délibérée et de défaillances accidentelles dans des systèmes de chiffrement (« goto fail ») ainsi que des vulnérabilités critiques dans des logiciels connus (Shellshock, Heartbleed, OpenSSL) ont laissé la communauté dubitative face à ces logiciels non vérifiés. La réaction a donc été de lancer des analyses indépendantes de la clé de ces logiciels ou que des chercheurs en sécurité les dissèquent à la recherche de vulnérabilités critiques (une alternative à l'analyse non officielle). Cela signifie que 2015 sera une autre année remplie de nouvelles vulnérabilités dangereuses qui apparaitront dans des anciens codes, exposant ainsi l'infrastructure Internet à des attaques.

4. Augmentation des attaques contre les distributeurs automatiques et les points de vente
Les attaques contre les distributeurs automatiques semblent avoir explosé cette année avec plusieurs incidents publics et la vive réaction des autorités à travers le monde pour faire face à cette crise. Une des conséquences de ces incidents est la prise de conscience que ces distributeurs automatiques sont très faciles à pirater et les cybercriminels l'ont bien remarqué. Comme la plupart de ces systèmes fonctionnent sous Windows XP et disposent d'une sécurité physique très faible, ils sont très vulnérables par défaut. Et comme les institutions financières disposent d'argent liquide, il est logique que les cybercriminels commencent par là.

En 2015, nous nous attendons à observer une évolution de ces attaques contre les distributeurs automatiques grâce à l'utilisation de techniques d'APT afin d'accéder au système d'information de ces machines. On verra ensuite les pirates compromettre les réseaux des banques et utiliser cet accès pour prendre le contrôle des distributeurs en temps réel.

5. Attaques Mac : des botnets OS X
Malgré les efforts d'Apple pour verrouiller le système d'exploitation Mac, nous continuons d'observer des logiciels malveillants envoyés via des torrents ainsi que des logiciels piratés. La popularité grandissante des appareils Mac OS X fait tourner les têtes dans le monde criminel et rend très intéressante la création de malwares pour cette plateforme. L'écosystème fermé par défaut empêche les malwares d'envahir la plate-forme mais certains utilisateurs choisissent de désactiver les mesures de sécurité Mac OS X surtout ceux qui utilisent des logiciels piratés. Cela signifie que ceux qui cherchent à pirater les systèmes OS X pour diverses raisons savent qu'ils ont juste à cacher leur malware dans un logiciel attirant (certainement en le faisant passer pour un générateur de clé) pour réussir à le diffuser. À cause des idées reçues sur la plateforme OS X, ces systèmes ont peu de chances d'avoir une solution antimalware qui détectera les infections une fois le malware installé : ce dernier passera donc inaperçu pendant très longtemps.

6. Des attaques contre les systèmes de billetterie automatique
Les incidents comme le piratage NFC contre les transports publics chiliens (http://securelist.com/blog/virus-watch/67283/android-nfc-hack-allow-users-to-have-free-rides-in-public-transportation) montre l'intérêt que les criminels ont pour les ressources publiques comme les systèmes de transports publics. Certains pirates ne chercheront même pas à obtenir de l'argent pour ce type d'attaques et seront simplement contents de voyager gratuitement et de partager leur technique avec d'autres. Bien que ces systèmes de billetterie soient vulnérables (la plupart d'entre eux fonctionnent sous Windows XP), dans de nombreuses villes, ils gèrent directement des transactions par carte bancaire. Nous nous attendons donc à voir des attaques plus violentes contre ces systèmes que cela soit pour détourner le système ou voler des données de carte bancaire.

7. Des attaques contre les systèmes de paiement virtuel
La logique veut que les cybercriminels cherchent à gagner de l'argent grâce à leurs attaques de la manière la plus efficace et la plus simple possible. Quoi de mieux que les systèmes de paiement virtuel qui n'en sont encore qu'à leurs débuts ? Nous nous attendons donc à ce que les criminels se jettent sur toutes les opportunités qu'ils trouveront pour exploiter ces systèmes. Qu'il s'agisse d'ingénierie sociale, d'attaques ciblant les appareils des utilisateurs (dans la plupart des cas, les téléphones mobiles), ou de pirater directement des banques, les cybercriminels choisiront les attaques qui pourront leur rapporter de l'argent rapidement et les systèmes de paiement virtuel finiront par en faire les frais.

Ces craintes peuvent également s'appliquer à Apple Pay qui utilise la NFC (Near Field Communications) pour gérer les transactions sans fil des utilisateurs.

8. Apple Pay
De précédentes attaques se sont concentrées sur les systèmes de paiement NFC mais, grâce à son adoption limitée, ces attaques n'ont pas rapporté beaucoup. Apple Pay va certainement changer cela. L'enthousiasme pour ce nouveau système de paiement va faire exploser l'adoption de ce système et cela attirera bien évidemment les cybercriminels qui chercheront à intercepter ces transactions. Le design d'Apple se concentre principalement sur la sécurité (avec par exemple, la virtualisation des données de transaction) mais nous sommes très curieux de voir comment les pirates exploiteront les fonctionnalités de ce système.

9. Compromettre l'Internet des objets
Les attaques contre l'Internet des objets (ou objets connectés) se sont limitées aux prototypes et aux avertissements (parfois exagérés) annonçant que les smart TV et les réfrigérateurs seront ciblés par les pirates pour créer des Botnets ou lancer des attaques malveillantes.
Alors que de plus en plus d'appareils connectés sont disponibles, nous nous attendons à observer un débat plus important sur la sécurité et la confidentialité, surtout parmi les entreprises de ce secteur. En 2015, on verra certainement des attaques contre des imprimantes connectées en réseau et autres appareils connectés qui aideront les pirates expérimentés à s'infiltrer dans les réseaux corporatifs. Nous nous attendons à ce que les appareils de l'Internet des objets fassent partie de l'arsenal des groupes utilisant les APT, surtout si l'on considère que la connectivité est désormais introduite aux procédés industriels ainsi qu'aux procédés de fabrication.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.economiematin.fr/news-2015-attaque-hacker-piratage-criminel-brulez
Par Nicolas Brulez

Quand la technologie nous fait rêver : Fujitsu invente l’écran tactile sans écran

	Quand la technologie nous fait rêver : Fujitsu invente l’écran tactile sans écran

Aucun réel rapport avec la cybercriminalité et la protection des données personnelles, mais je ne peux rester insensible, lorsque la technologie m'impressionne. C'est une forme de morceau choisi de la technologie que j'avais envie de partager, avec vous : un écran tactile… sans écran, le papier tactile !

Fujitsu Laboratories has developed a next generation user interface which can accurately detect the users finger and what it is touching, creating an interactive touchscreen-like system, using objects in the real word.

« We think paper and many other objects could be manipulated by touching them, as with a touchscreen. This system doesn't use any special hardware; it consists of just a device like an ordinary webcam, plus a commercial projector. Its capabilities are achieved by image processing technology. »

Using this technology, information can be imported from a document as data, by selecting the necessary parts with your finger.

This technology measures the shape of real-world objects, and automatically adjusts the coordinate systems for the camera, projector, and real world. In this way, it can coordinate the display with touching, not only for flat surfaces like tables and paper, but also for the curved surfaces of objects such as books.

« Until now, gesturing has often been used to operate PCs and other devices. But with this interface, we're not operating a PC, but touching actual objects directly, and combining them with ICT equipment. »

« The system is designed not to react when you make ordinary motions on a table. It can be operated when you point with one finger. What this means is, the system serves as an interface combining analog operations and digital devices. »

To detect touch accurately, the system needs to detect fingertip height accurately. In particular, with the low-resolution camera used here (320 x 180), if fingertip detection is off by a single pixel, the height changes by 1 cm. So, the system requires technology for recognizing fingertips with high precision.

« Using a low-res webcam gives a fuzzy picture, but the system calculates 3D positions with high precision, by compensating through image processing. »

This system also includes technology for controlling color and brightness, in line with the ambient light, and correcting for individual differences in hand color. In this way, it can identify fingertips consistently, with little influence from the environment or individual differences.

Also, in situations that don't use touch, the system can be operated by gesturing. In this demo, when you move your fist, you can manipulate the viewpoint for 3D CAD data. So, there could be applications for this touch system by combining it with current gesture systems.

« For example, we think this system could be used to show detailed information at a travel agent's counter, or when you need to fill in forms at City Hall. »

« We aim to develop a commercial version of this system by fiscal 2014. It's still at the demonstration level, so it's not been used in actual settings. Next, we'd like to get people to use it for actual tasks, see what issues arise, and evaluate usability. We want to reflect such feedback in this system. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://mashable.com/2013/04/16/fujitsu-paper-touchscreen/
http://www.diginfo.tv/v/13-0025-r-en.php