FIC 2016 – Demandez le programme…

FIC 2016 – Demandez le programme…

Les données sont le carburant de la transformation numérique de nos sociétés. Elles irriguent désormais l'ensemble des réseaux et systèmes d'information et, à travers eux, des activités humaines. Les chiffres donnent le vertige : 144 milliards de mails sont échangés dans le monde chaque jour, 30 gigaoctets sont publiés chaque seconde, 800 000 nouveaux sites web apparaissent quotidiennement, la quantité d'informations disponibles double tous les deux ans…. avec seulement 42 % de la population mondiale connectée.

Le thème du FIC 2016 :
Malgré cette croissance exponentielle, les données restent un capital fragile. Il faut en effet susciter les conditions de leur création, puis les entretenir, les enrichir, les transformer, les valoriser et les protéger pour en faire une source de progrès pour l'Homme. Les défis sont donc multiples. Au plan stratégique, tout d'abord : le primat accordé par l'Union européenne aux données personnelles serait-il donc incompatible avec le « business » de la donnée ? Au plan juridique, également : comment concilier l'imbrication croissante des données et l'application de la notion de propriété ? Au plan sécuritaire, enfin : comment créer le climat de confiance propice au développement de nouveaux usages pour le citoyen, l'entreprise, la collectivité territoriale, l'Etat ?

Programme FIC 2016 Lundi 25 janvier 2016

lundi 10:00 – 11:00|Séance plénière VA-T-ON VERS UNE CRISE DE CONFIANCE DES UTILISATEURS ?
lundi 11:00 – 11:30|Séance plénière ALLOCUTION DE GÜNTHER OETTINGER, COMMISSAIRE EUROPÉEN CHARGÉ DE L'ÉCONOMIE ET DE LA SOCIÉTÉ NUMÉRIQUES
DT01|lundi 12:00 – 12:30|Démonstration technique INFOBLOX – CIBLE D'ATTAQUES ET VECTEUR D'EXFILTRATION DE DONNÉES : VOTRE DNS EST VULNÉRABLE !
C01|lundi 12:15 – 13:00|Conférence ANSSI – BSI : CYBERSÉCURITÉ : LA COOPÉRATION FRANCO-ALLEMANDE
C02|lundi 12:15 – 13:00|Conférence SOPRA-STERIA – PROTÉGER LES SUPPLY CHAIN DES SECTEURS ÉCONOMIQUES SENSIBLES AVEC L'INNOVATION BOX@PME
C03|lundi 12:15 – 13:00|Conférence THALES – PROTECTION DES DONNÉES ET TRANSFORMATION NUMÉRIQUE
C05|lundi 12:15 – 13:00|Conférence QUALYS – TÉMOIGNAGE CLIENT DÉFENSE
FT01|lundi 12:15 – 12:30|FIC Talk RSA – INTELLIGENCE DRIVEN SECURITY » : L'UTILISATEUR EST LE NOUVEAU PÉRIMÈTRE
DT02|lundi 12:30 – 13:00|Démonstration technique NES – LE SOC 'INTELLIGENT' : OU COMMENT APPRÉHENDER LA DÉMARCHE D'UN HACKER
FT02|lundi 12:30 – 12:45|FIC Talk CONTEXTUAL SECURITY INTELLIGENCE
MC01|lundi 12:30 – 12:45|Master class DE FRUTAS À ALIENSPY, ANALYSE D'UNE FAMILLE DE RAT JAVA
DT03|lundi 13:00 – 13:30|Démonstration technique IMS NETWORKS – ANTI DDOS AS A SERVICE
TV03|lundi 13:00 – 13:05|Plateau TV LES RÉSEAUX ÉLECTRIQUES INTELLIGENTS.
DT04|lundi 13:30 – 14:00|Démonstration technique CONIX – VERS UN DÉVELOPPEMENT D'OUTILS INNOVANTS EN MODE AGILE EN RÉPONSE À LA CYBER-MENACE
A05|lundi 14:00 – 15:30|Agora ETHIQUE ET CYBERESPACE
A09|lundi 14:00 – 15:30|Atelier PROCÈS SIMULÉ SUR UNE FUITE DE DONNÉES CONFIDENTIELLES
DT05|lundi 14:00 – 14:30|Démonstration technique BACKBOX- AUTOMATING NETWORK AND SECURITY DEVICE OPERATIONS
A01|lundi 14:30 – 15:30|Atelier LA NOUVELLE CYBERCRIMINALITÉ LIÉE AUX DONNÉES
A02|lundi 14:30 – 15:30|Atelier INTERNET DES OBJETS : LA NOUVELLE FRAGILITÉ ?
A03|lundi 14:30 – 15:30|Atelier INCIDENT DE SÉCURITÉ : COMMENT PRENDRE EN COMPTE TOUTES LES CONTRAINTES ?
A04|lundi 14:30 – 15:30|Atelier COMPRENDRE ET ORGANISER SES DONNÉES
A06|lundi 14:30 – 15:30|Atelier CYBERSÉCURITÉ ET OIV : QUELLES OBLIGATIONS ?
A07|lundi 14:30 – 15:30|Atelier EXTERNALISATION DU SOC : QUELS AVANTAGES POUR QUELS RISQUES ?
A08|lundi 14:30 – 15:30|Atelier THE CYBER GAME
A10|lundi 14:30 – 15:30|Atelier LES NOUVEAUX MÉTIERS LIÉS AUX DONNÉES
A11|lundi 14:30 – 16:00|Atelier CLUSTERS ET CYBERSÉCURITÉ : COMMENT SOUTENIR LE DÉVELOPPEMENT DE LA FILIÈRE ?
MC03|lundi 14:30 – 15:15|Master class LES TECHNIQUES SPÉCIALES D'ENQUÊTE
DT06|lundi 15:00 – 15:30|Démonstration technique SECLAB – TIXEO : VISIOCONFÉRENCE SÉCURISÉE ENTRE SYSTÈMES NON CONNECTÉS
DT07|lundi 15:30 – 16:00|Démonstration technique BITDEFENDER – COMMENT GARANTIR LA CONTINUITÉ DES SERVICES DE SÉCURITÉ
MC04|lundi 15:30 – 16:15|Master class UTILISATION OPÉRATIONNELLE DES TECHNIQUES D'EXTRACTION DE CONNAISSANCE (DATAMINING, BIG DATA) DANS LE RENSEIGNEMENT ET LA CONCEPTION D'ATTAQUES
TV06|lundi 15:30 – 15:40|Plateau TV LES NOUVELLES CONNAISSANCES EN NEUROSCIENCES, SCIENCES ET THÉRAPIES COGNITIVES PEUVENT ELLES AIDER À MIEUX COMPRENDRE ET GÉRER LA CYBER SÉCURITÉ ?
C07|lundi 16:00 – 16:45|Conférence INEO – RETOUR D'EXPÉRIENCE D'UN LEADER DE LA GRANDE DISTRIBUTION EN MATIÈRE DE GESTION GLOBALE DU CYBER-RISQUE
C08|lundi 16:00 – 16:45|Conférence PÔLE D'EXCELLENCE CYBER – EXPÉRIMENTER AVEC SON CLIENT : EXEMPLES EN SANTÉ, CHIMIE ET DÉVELOPPEMENT LOGICIEL
C09|lundi 16:00 – 16:45|Conférence HARMONIE TECHNOLOGIE – EXTERNALISATION DES DONNÉES, PANORAMA DE MENACES ET ORIENTATIONS 2016
C10|lundi 16:00 – 16:45|Conférence PWC
DT08|lundi 16:00 – 16:30|Démonstration technique TIXEO – DÉMONSTRATION DE LA SOLUTION DE VISIOCONFÉRENCE HAUTEMENT SÉCURISÉ TIXEO
FT04|lundi 16:00 – 16:15|FIC Talk SOLUTION ANTI D-DOS, OÙ VONT MES DONNÉES ?
FT05|lundi 16:15 – 16:30|FIC Talk CLOUD – COMMENT MÉRITER LA CONFIANCE À L'HEURE DE LA REMISE EN CAUSE SAFE HARBOR ?
MC05|lundi 16:15 – 17:00|Master class IMPUTABILITÉ DES CONNEXIONS INTERNET EN ENTREPRISE : PROBLÉMATIQUES TECHNIQUES ET RÉGLEMENTAIRES. RETOUR D'EXPÉRIENCE SUR LE PROJET LIBRE ALCASAR
DT09|lundi 16:30 – 17:00|Démonstration technique HEXATRUST – BERTIN IT – SENTRYO – CYBERSÉCURITÉ INDUSTRIELLE : 6 MESURES D'HYGIENE A PRENDRE EN 2016
FT06|lundi 16:30 – 16:45|FIC Talk 2020 NEW TECHNOLOGIES, NEW HOPES, NEW CHALLENGES
DT10|lundi 17:00 – 17:30|Démonstration technique HEXATRUST – WALLIX / ITRUST – FUITE DE VOS DONNÉES SENSIBLES, COMMENT VOUS PRÉMUNIR ET IDENTIFIER LES COMPORTEMENTS À RISQUES DES UTILISATEURS ?
TV08|lundi 17:00 – 17:05|Plateau TV
P02|lundi 17:15 – 18:15|Séance plénière DONNÉES : UNE CHANCE POUR L'EUROPE

Programme FIC 2016 Mardi 26 janvier 2016

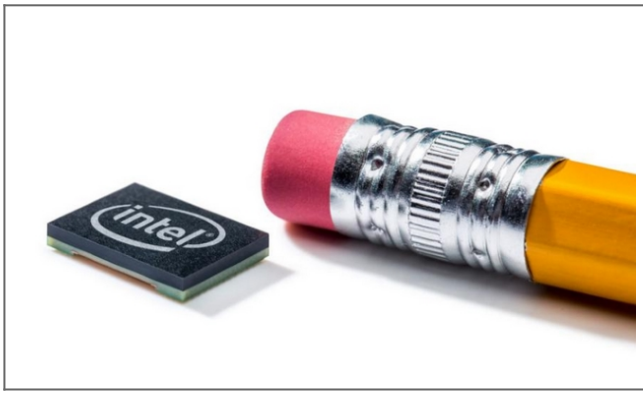
mardi 09:00 – 09:30|Séance plénière ALLOCUTION DE MONSIEUR BERNARD CAZENEUVE, MINISTRE DE L'INTÉRIEUR, RÉPUBLIQUE FRANÇAISE
P03 mardi 09:30 – 10:30|Séance plénière QUELLE SOUVERAINETÉ SUR LES DONNÉES ?
B01 mardi 11:00 – 12:00|Atelier DATA 2030
B02 mardi 11:00 – 12:00|Atelier RÈGLEMENT E-IDAS : UNE RÉELLE OPPORTUNITÉ POUR L'INDUSTRIE EUROPÉENNE DE LA CONFIANCE NUMÉRIQUE
B03 mardi 11:00 – 12:00|Atelier L'USINE DU FUTUR : QUELS RISQUES ?
B04 mardi 11:00 – 12:00|Atelier LA GESTION DES CRISES CYBER
B05 mardi 11:00 – 12:00|Atelier COMMENT ASSURER SES DONNÉES ?
B06 mardi 11:00 – 12:00|Agora CYBERSÉCURITÉ ET FRANCOPHONIE
B07 mardi 11:00 – 12:00|Atelier LES APT EN MILIEU MILITAIRE
B08 mardi 11:00 – 12:00|Atelier DATA LOSS PREVENTION : ENFIN QUELQUES SOLUTIONS MATURES ?
B09 mardi 11:00 – 12:00|Atelier SMART GRID : QUELLES VULNÉRABILITÉS ?
B10 mardi 11:00 – 12:00|Atelier SANTÉ : LA CYBERSÉCURITÉ VITALE
DT11 mardi 11:00 – 11:30|Démonstration technique PALO ALTO NETWORKS – DE LA RÉSILIENCE À LA PRÉVENTION DE LA CYBERCRIMINALITÉ
MC06 mardi 11:00 – 11:45|Master class POURQUOI SÉCURISER L'IMPLÉMENTATION DES ALGORITHMES CRYPTOGRAPHIQUES ?
MC07 mardi 11:00 – 11:45|Master class DONNÉES PERSONNELLES ET OBJETS CONNECTÉS : ATTAQUES, DÉFENSE ET CONTRE-MESURES
DT12 mardi 11:30 – 12:00|Démonstration technique HEXATRUST – ILEX . INWEBO / OPENTRUST – GESTION DES IDENTITÉS ET DES ACCÈS : LA RÉPONSE CONCRÈTE ET ILLUSTRÉE D'HEXATRUST
DT13 mardi 12:00 – 12:30|Démonstration technique HEXATRUST – DENYALL / NETHEOS – SÉCURISATION DES TRANSACTIONS : UN ENJEU VITAL À L'HEURE DU DIGITAL
MC08 mardi 12:00 – 12:45|Master class LA FAILLE LOGJAM
DT14 mardi 12:30 – 13:00|Démonstration technique HEXATRUST – IDECSI / VADERETRO – APPLICATION CENTRALE ET AU CŒUR DU RISQUE : QUELLES SOLUTIONS POUR PROTÉGER LA MESSAGERIE ?
DT15 mardi 13:00 – 13:30|Démonstration technique HEXATRUST – THEGREENBOW / PRIM'X – CHIFFRER LES DONNÉES – TOUJOURS PAS UN REFLEXE NATUREL ?
TV11 mardi 13:00 – 13:10|Plateau TV
C11 mardi 13:30 – 14:15|Conférence ORANGE CYBERDEFENSE – CAC 40 : RETOUR SUR LES PROBLÉMATIQUES DE SÉCURITÉ EN ENTREPRISE
C12 mardi 13:30 – 14:15|Conférence KASPERSKY – ANALYSE DE L'ATTAQUE AVANCÉE DUQU 2.0
C13 mardi 13:30 – 14:15|Conférence TÉMOIGNAGE DU MINISTERE DE L'ÉDUCATION NATIONALE – SÉCURISATION DES CENTRES DE DONNÉES
C14 mardi 13:30 – 14:15|Conférence MINISTÈRE DE LA DÉFENSE – ECHANGE DE POINT DE VUE SUR LA FORMATION ET ENTRAÎNEMENT
C15 mardi 13:30 – 14:15|Conférence TREND MICRO – TÉMOIGNAGE DU GROUPE KEOLIS – UNIFORMISER SES SOLUTIONS DE SÉCURITÉ POUR MIEUX LUTTER CONTRE LES NOUVELLES MENACES
DT16 mardi 13:30 – 14:00|Démonstration technique HEXATRUST – ERCOM / PRADEO – PROTECTION DES FLUX MOBILES ET WEB : LA CLÉ DE VOUTE DU DÉVELOPPEMENT DE L'ÉCONOMIE DIGITAL
FT07 mardi 13:30 – 13:45|FIC Talk QUALYS – ADOPTEZ UNE STRATÉGIE CONTRE LES MENACES
MC09 mardi 13:30 – 14:15|Master class IOT, SERRURES CONNECTÉES ET SÉCURITÉ DU CONTRÔLE D'ACCÈS ÉLECTRONIQUE
MC10 mardi 13:30 – 14:15|Master class LA TECHNOLOGIE FROGANS SÉCURISE LA PUBLICATION DE DONNÉES SUR L'INTERNET
FT09 mardi 14:15 – 14:30|FIC Talk ET SI LA SÉCURITÉ ÉTAIT EN RÉALITÉ LE PRINCIPAL ENJEUX DE L'INTERNET DES OBJETS ?
DT17 mardi 14:30 – 15:00|Démonstration technique SPLUNK – IDENTIFICATION ET ANALYSE DES COMPORTEMENTS DÉVIANTS PAR LE MACHINE LEARNING
TV12 mardi 14:30 – 14:40|Plateau TV E-DISCOVERY OR FORENSIC : HOW TO DEAL WITH LEGAL PRIVILEGE AND PERSONAL INFORMATION
B11 mardi 14:45 – 15:45|Atelier INVESTIGATIONS DANS LE CYBERESPACE : LES TECHNIQUES D'ENQUÊTE AU REGARD DE LA PROTECTION DE LA VIE PRIVÉE ?
B12 mardi 14:45 – 15:45|Atelier PEUT-ON PARLER DE THÉÂTRE D'OPÉRATIONS CYBER ?
B13 mardi 14:45 – 15:45|Atelier LE MARCHÉ EUROPÉEN DU NUMÉRIQUE : CHIMÈRE OU RÉELLE OPPORTUNITÉ ?
B14 mardi 14:45 – 15:45|Atelier BIG DATA : L'OUTIL SÉCURITAIRE ULTIME
B15 mardi 14:45 – 15:45|Atelier ANALYSE FORENSIQUE : LES NOUVEAUX DÉFIS
B16 mardi 14:45 – 15:45|Atelier CYBER THREAT INTELLIGENCE : ENTRE MYTHES ET RÉALITÉ
B17 mardi 14:45 – 15:45|Atelier COMMENT RÉUSSIR LE DÉPLOIEMENT D'UN SECURITY OPERATION CENTER ?
B18 mardi 14:45 – 15:45|Atelier QUEL RÔLE POUR LES COLLECTIVITÉS TERRITORIALES DANS LES SMART CITY ?
B19 mardi 14:45 – 15:45|Atelier RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES : QUELLES CONSÉQUENCES ?
B20 mardi 14:45 – 15:45|Atelier DE LA NÉCESSITÉ DE SÉCURITÉ DANS LES TRANSPORTS INTELLIGENTS : CHALLENGES ET SOLUTIONS
MC11 mardi 14:45 – 15:30|Master class AN APPROACH TO SHARED DATA TRACEABILITY
MC12 mardi 14:45 – 15:30|Master class DE L'HAMEÇONNAGE CIBLÉ À LA COMPROMISSION TOTALE DU DOMAINE : DÉMONSTRATION ET LIMITATION DES RISQUES
DT18 mardi 15:00 – 15:30|Démonstration technique DARKTRACE – L'ENTERPRISE IMMUNE SYSTEM : » COMMENT UTILISER L'AUTO-APPRENTISSAGE POUR LA DÉTECTION DES MENACES À L'INTÉRIEUR DU RÉSEAU ?
TV13 mardi 15:00 – 15:05|Plateau TV PRÉSENTATION DES PROJETS EUROPÉENS «ORIGIN » ET «EKSITENZ »
DT19 mardi 15:30 – 16:00|Démonstration technique SECLAB – PROTECTION TOTALE HARDWARE CONTRE LES ATTAQUES USB
TV14 mardi 15:30 – 16:00|Plateau TV NEUROSCIENCES ET ERGONOMIE PEUVENT-ELLES CONTRIBUER À RÉDUIRE LE RISQUE HUMAIN EN CYBER SÉCURITÉ ?
C16 mardi 16:15 – 17:00|Conférence PRÉSENTATION DU PROGRAMME EUROPÉEN DE RECHERCHE ET D'INNOVATION EN SÉCURITÉ : HORIZON 2020 SOCIÉTÉS SÛRES.
C17 mardi 16:15 – 17:00|Conférence MICROSOFT – PROTÉGEZ VOS ACTIFS PAR LE BIAIS DE LA CLASSIFICATION DE L'INFORMATION
C18 mardi 16:15 – 17:00|Conférence OTAN – RENFORCER LA CYBERDÉFENSE DE L'OTAN : DU SOMMET DE GALLES À CELUI DE VARSOVIE
FT10 mardi 16:15 – 16:35|Conférence PANORAMA DE LA CYBERCRIMINALITÉ
DT21 mardi 16:30 – 17:00|Démonstration technique DELL – DATA SECURITY SOLUTIONS : UNE PROTECTION DE NOUVELLE GÉNÉRATION CONTRE LES MENACES
TV16 mardi 16:30 – 16:40|Plateau TV TRAITEMENT JUDICIAIRE DE LA CYBERCRIMINALITÉ

Lien vers le site officiel
Programme FIC 2016 jour 1
https://www.forum-fic.com/site/FR/Programme/Jour_1
Programme FIC 2016 jour 2
https://www.forum-fic.com/site/FR/Programme/Jour_2
FIC 2016 Inscrivez-vous / Enregistrez-vous

Réagissez à cet article

Source : *FIC 2016*

Intel veut encore et toujours que vous enfiliez un ordinateur

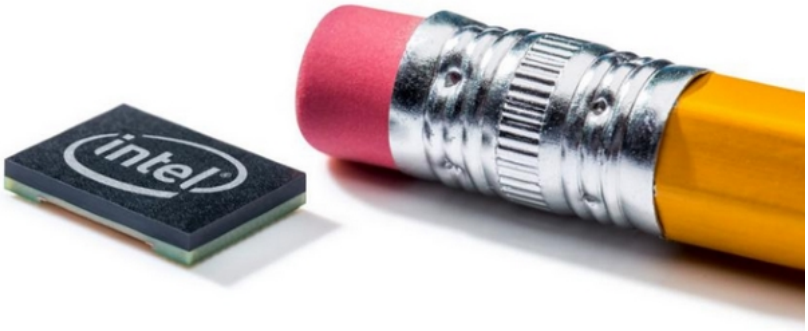


Intel veut encore et toujours que vous enfiliez un ordinateur

---

Si les objets connectés connaissent des fortunes variables, Intel creuse le sillon des wearables et met à disposition des constructeur son module Curie, un ordinateur miniature équipé de capteurs de mouvements.

Intel annonce être prêt à livrer Curie, un petit ordinateur qui pourrait aider les wearables dans leur quête de minceur. Le PDG d'Intel Brian Krzanich a annoncé lors de la keynote de la société au CES que Curie serait disponible au premier trimestre de cette année, et couterait moins de 10 dollars l'unité.



L'ordinateur Curie d'Intel, destiné au marché des wearables. (Source : Intel)

Présenté l'an passé à Las Vegas, Curie est un micro ordinateur portable qui tient littéralement dans un bouton de veste. Le PDG d'Intel en avait fait la démonstration lors de la keynote de l'édition précédente. Le tout petit ordinateur Curie est un enjeu capital pour Intel et le secteur des wearables. Protocole de communication Bluetooth, accéléromètre, gyroscope ; Intel assure que Curie possède également une batterie de longue durée de la taille « d'une pièce de monnaie ». De quoi assurer un fonctionnement constant.
Le module Curie est équipé également d'un processeur 32-bit Intel Quark, de 384ko de mémoire flash, de 80ko de SRAM et de capteurs DSP.

Diminuer la taille des équipements

De quoi aussi diminuer sensiblement la taille des équipements électroniques qui équipent montres et bijoux connectés, mais aussi proposer des fonctionnalités de suivi de la santé des utilisateurs sur des vêtements sans les déformer pour autant. Surtout, le coût additionnel de ces produits connectés serait modique.
A titre d'exemple, le PDG d'Intel a présenté sur scène deux cyclistes BMX dont la selle et le guidon de leur vélo sont équipés d'un module Curie rapporte Technology Review. Leurs cascades réalisées en direct étaient ainsi analysées en temps réel et retransmises sur un écran géant. Et si Intel se concentre si fort sur le marché des wearables, c'est qu'il s'agit pour lui d'un enjeu majeur pour enfin trouver grâce aux yeux du marché de la mobilité.

Un marché en croissance et déjà embouteillé

A noter qu'Intel est loin d'être le seul a se positionner sur le segment des composants pour wearables.Samsung vient par exemple de présenter un processeur. Côté marché, la baisse des prix provoque un certain engouement des consommateurs. L'Idate prévoit que 123 millions de wearables seront vendus en 2018.
En France, Cityzen Sciences aurait levé 100 millions d'euros en 2015 pour développer des capteurs à destination des vêtements.

Réagissez à cet article

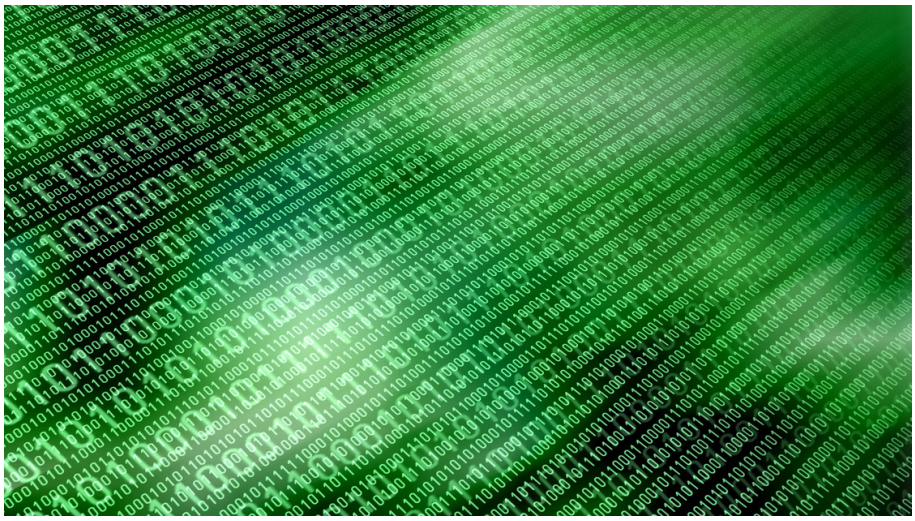
Source : *Intel veut encore et toujours que vous enfiliez un ordinateur*

Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

	Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

---

Le Département des Alpes-Maritimes ,1er organisme français à obtenir le Label Gouvernance Informatique et Libertés de la CNIL.



Le Département a depuis longtemps intégré le numérique comme nouvelle dimension de la vie de l'usager. Il s'est ainsi engagé formellement dans le respect du droit des personnes au travers de la mise en oeuvre d'un cadre de confiance autour de l'économie numérique en établissant une politique de gestion des données à caractère personnel. Un engagement récompensé au niveau national pour la première fois en France.
Le 22 octobre 2015, la CNIL a délivré au Département des Alpes-Maritimes le premier Label Gouvernance Informatique et Libertés tous secteurs confondus. L'obtention de ce label vient récompenser le travail des services départementaux, ainsi que l'attachement éthique du Département à la protection des données relatives aux usagers ou à celles de ses agents.
Cette distinction et les bonnes pratiques qui en découlent, illustrent ainsi, à juste titre, le comportement responsable et loyal que la collectivité a engagé en matière de réalisation et d'exploitation des données à caractère personnel.
Le Lab 06 a ouvert ses portes le 25 septembre 2015 au cœur du Centre administratif départemental. Il incarne la volonté du Département des Alpes-Maritimes de s'engager davantage dans la voie de la transformation numérique avec la création de #E-zy06 dont l'ambition est d'offrir un service public encore plus accessible quelle qu'en soit la modalité : physique, téléphonique ou numérique.
L'objectif est de faire des Alpes-Maritimes un département pionnier dans le numérique, capable d'apporter le plus grand service aux usagers.

Réagissez à cet article

Source : *La politique départementale de sécurité des données personnelles saluée par la CNIL – Département des Alpes-Maritimes*

Critical Infrastructure Sectors of Nations facing cybercrime

Critical Infrastructure Sectors of Nations facing cybercrime

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.
PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector
The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century.

Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

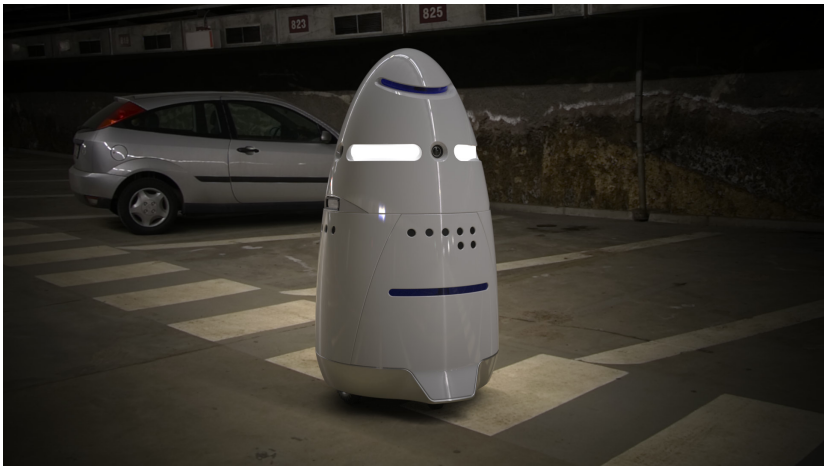
Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Réagissez à cet article

Source : *Critical Infrastructure Sectors | Homeland Security*

Des robots sentinelle contre le crime dans la Silicon Valley



Des robots sentinelle contre le crime dans la Silicon Valley

Une start-up de Palo Alto, Knightscope, déploie dans les rues de la Silicon Valley des robots pour lutter contre le crime.

Non, ce n'est pas le pitch d'un nouveau film d'anticipation ou de science-fiction, mais bien une réalité d'aujourd'hui. Ces robots, les Knightscope K5 Security Robot, sont déjà dans les rues et patrouilles pour dissuader ou récolter des données.

Bardés de capteurs

Ces robots ne sont pas armés, ce qui pourrait arriver aux États-Unis vu les lois en vigueur dans certains états. Par contre, ils sont équipés de multiples capteurs qui leur permettent de voir à 360°, d'entendre, de sentir et de ressentir. Le système de guidage et de pilotage est le même que celui des Google Car.

Ils mesurent un peu plus d'un mètre cinquante, pèsent près de 137 kg, sont de forme ovoïde et de couleur blanche. Ils téléchargent en temps réel ce qu'ils voient et entendent et sont conçus pour réagir à des bruits significatifs comme le bris de glace ou des coups de feu. Si cela se produit, le K5 enregistre alors beaucoup d'informations sur son environnement comme la géolocalisation, photos, vidéos, plaques d'immatriculation des véhicules à proximité et même les visages des personnes proches dans l'éventualité d'une reconnaissance faciale.

Les K5 peuvent donner l'alerte aux autorités compétentes en cas de « détection » crime via une plateforme Internet accessibles aux forces de l'ordre.

Le K5 est déjà en fonction dans des centres commerciaux ou des campus universitaires comme assistant de sécurité et, selon Stacy Stephens cofondatrice de Knightscope, ils ont un très bon accueil et reçoivent même des câlins.

Le business model de Knightscope pour les K5 est MaaS, Machine-as-a-Service, et coûte 4 500 dollars par mois, pour un service 24h/24 et 7jr/7 soit 6,25 dollars de l'heure.

Toutes ressemblances avec Dalek de Docteur Who est fortuite…

Réagissez à cet article

Source : *Des robots contre le crime dans la Silicon Valley – Ere Numérique*

Comment protéger les données de vos enfants des pirates informatiques

Comment protéger les données de vos enfants des pirates informatiques

---

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Après l'annonce du piratage début novembre de VTech, le leader mondial des tablettes ludo-éducatives, c'est maintenant au tour d'Hello Kitty d'être accusée de mal sécuriser les données de ses utilisateurs. Pendant près d'un mois, les données personnelles de 3,3 millions de membres de la communauté en ligne du fabriquant japonais Hello Kitty (dont, évidement, beaucoup d'enfants) auraient été exposées en raison d'une faille de sécurité.

A quelques jour de Noël, ces deux affaires montrent clairement à quel point il est facile aujourd'hui pour les hackeurs de dérober des informations sensibles.Et aussi le danger qui peut en découler, comme le rappelle à metronews la Commission nationale de l'informatique et des libertés (CNIL) : « Nous constatons que certains secteurs industriels ajoutent une connectivité à leurs produits sans disposer historiquement d'une culture en sécurité informatique ».

► Vérifiez si votre mail est piraté
Il existe un moyen simple de savoir si votre adresse mail a été touchée. Pour cela, il faut se rendre sur le site haveibeenpwned.com. Entrez votre adresse mail, puis cliquez sur « pwned ? » pour lancer la recherche.
► Changez votre mot de passe
Par précaution, il est recommandé aux utilisateurs des services qui ont connu des intrusions de ce genre de changer leurs mots de passe. « Il doit être composé d'au moins 3 types de caractères différents parmi les quatre types de caractères existants : majuscules, minuscules, chiffres et caractères spéciaux ». Pour en savoir plus, rendez-vous sur le site de la CNIL.
► Ne communiquez que le minimum d'infos
Pour les enfants (et leurs parents), la CNIL recommande ainsi d'utiliser des pseudonymes sur les services en lignes, et de ne communiquer que le minimum d'informations. Par exemple, saisissez une date de naissance au 1er janvier si le système a besoin d'une indication de tranche d'âge.
► Veillez à bien lire les conditions d'utilisation
Outre les risques de sécurité révélés par la faille VTech, les parents doivent être vigilants concernant les possibilités de réutilisation des données collectées (profilage publicitaire) et s'assurer de la possibilité d'y accéder et de les supprimer.

Réagissez à cet article

Source : *Piratages VTech et Hello Kitty : comment protéger les données de vos enfants – metronews*

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

---

 **Le mois dernier, une cyberattaque contre des fournisseurs d'énergie ukrainiens avait privé 80 000 clients d'électricité. D'après la signature du malware, l'attaque avait été imputée à un groupe de pirates ayant des liens avec la Russie. Mais, selon une nouvelle étude, le malware n'est pas directement à l'origine de la panne : les assaillants sont intervenus physiquement pour activer les disjoncteurs et provoquer la coupure de courant.**

Selon des informations publiées samedi par l'équipe du SANS Industrial Control Systems (ICS), une organisation spécialisée dans l'information et la formation des professionnels de la sécurité, le malware a bien servi aux pirates à s'introduire dans le réseau des fournisseurs d'électricité, mais ils sont ensuite intervenus sur les disjoncteurs pour couper l'alimentation. Depuis des années, les experts mettent en garde sur la vulnérabilité des systèmes de contrôle industriels. Les cyberattaques survenues le 23 décembre contre les installations ukrainiennes montrent que leurs craintes sont justifiées. Selon les experts du #SANS ICS, ces évènements sont aussi la preuve que de telles attaques sont planifiées et très coordonnées.
Depuis l'annexion de la Crimée par la Russie en 2014, les tensions entre la fédération et l'Ukraine restent fortes. « Pour masquer le piratage et l'intrusion dans les réseaux, les agresseurs sont intervenus physiquement sur la centrale électrique », a déclaré l'équipe du SANS ICS. « Les agresseurs ont également lancé en simultané une attaque DDoS par déni de service sur le réseau téléphonique afin de bloquer les appels des clients affectés par la panne », a encore déclaré l'organisation. Les attaques auraient visé les deux fournisseurs d'énergie Prykarpattyaoblenergo et Kyivoblenergo. Ce dernier a déclaré dans une mise à jour de service que 80 000 clients dépendant de 30 sous-stations avaient été déconnectés du réseau.

Des pannes provoquées par une action physique

Plusieurs entreprises de sécurité ont analysé le #malware Black Energy 3 et le #composant Killdisk utilisés pour les attaques. Jeudi dernier, l'entreprise de sécurité iSight Partners basée à Dallas a déclaré que ces logiciels malveillants avaient déjà été utilisés dans le passé par le #groupe de pirates Sandworm connu pour avoir de puissants intérêts russes. Mais, comme iSight, le SANS ICS pense que les pannes ne sont pas à mettre exclusivement sur le compte des malwares. « Autrement dit, de nouvelles preuves pourraient remettre en cause l'impact réel des composantes malveillantes impliquées dans l'attaque », a écrit Michael Assante, directeur du SANS ICS.
Le composant Killdisk écrase le Master Boot Record (MBR), premier secteur du disque dur chargé par le PC avant de monter le système d'exploitation, et empêche donc le PC de démarrer. Selon Symantec, Killdisk peut aussi écraser des fichiers en écrivant des données inutiles. Michael Assante avance que Killdisk n'était pas compatible avec le système SCADA de contrôle et d'acquisition de données utilisé par les deux opérateurs. Mais il a peut-être été utilisé pour effacer d'autres fichiers qui auraient permis la restauration des systèmes. « Il semble que les fournisseurs d'électricité ont rétabli leurs services en actionnant manuellement les disjoncteurs au bout de trois et six heures », a ajouté le directeur du SANS ICS. Selon lui, « il faudrait féliciter les opérateurs ukrainiens pour leur diligence et les efforts accomplis pour restaurer leurs services ».

Réagissez à cet article

Source : *Panne électrique en Ukraine : le malware n'est pas seul en cause – Le Monde Informatique*

Carte de paiement sans contact – Le client n’est pas toujours roi

Carte de paiement sans contact – Le client n’est pas toujours roi

---

Refuser les cartes bancaires équipées du paiement sans contact n’est pas toujours simple. Un client du Crédit agricole l’a appris à ses dépens.
En avril 2015, un adhérent de l’UFC-Que Choisir de Senlis saisit l’association locale de ses difficultés avec son agence du Crédit agricole de Rixheim (68). Celle-ci lui a adressé en renouvellement une carte bancaire Visa munie de la fonction paiement sans contact. Ayant lu dans Que Choisir que cette fonction n’était pas sans faille, ce consommateur demande à sa banque le remplacement de sa carte par une même carte Visa mais sans cette nouvelle fonction. Refus de son agence, puis de la direction régionale du Crédit agricole qui affirme que c’est impossible et lui propose en échange soit une carte Visa avec débit différé, soit un autre type de carte bancaire. Pas d’accord, le particulier fait part de ce blocage à l’association locale de l’UFC-Que Choisir de Senlis.

Client à la porte
L’intervention de cette dernière auprès de la banque n’aura pas plus de succès. Face à un tel refus, elle saisit la Cnil (Commission nationale de l’informatique et des libertés) au motif que le Crédit agricole viole une de ses recommandations qui impose aux banques d’offrir à leurs clients la possibilité de refuser la fonction paiement sans contact.
La Cnil rejette la plainte de l’association locale, déclarant ne pas pouvoir imposer aux banques un changement de carte à l’identique mais rappelle que le particulier a la possibilité de faire désactiver la fonction.
Fort de cette réponse, le consommateur demande à son agence cette désactivation.
Pour toute réponse, la banque a mis son client à la porte, le sommant de restituer tous ses moyens de paiement. La Cnil a été avertie d’un tel comportement.

Réagissez à cet article

Source : *Carte de paiement sans contact – Le Crédit agricole a la main leste – UFC Que Choisir*

FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données

	**#FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données**

Pendant longtemps, la sécurité des données se confondait avec celle de la sécurité des systèmes d'information. Or la décorrélation croissante entre le contenant (support physique ou applicatif) et le contenu en raison de l'émergence des technologies de virtualisation, du « cloud computing » et de nouveaux modèles économiques change aujourd'hui la donne. La donnée est devenue un « objet » à part entière qui s'appréhende indépendamment de son support.

Axe 1 : les données, carburant de la transformation numérique.

Les données sont omniprésentes et multiformes : on peut citer les données personnelles, sociales, médicales, bancaires, d'entreprises, de géolocalisation, de sécurité, de dossiers passagers (PNR) etc. Cette compartimentation en fonction des usages ou des secteurs d'activité a-t-elle cependant encore un sens ? Comment gérer l'information indépendamment des supports utilisés ? Au-delà de la métaphore, les données constituent-elles véritablement un « nouvel or noir » ?

Axe 2 : la maitrise des données, enjeu de souveraineté

Posséder une « industrie de la donnée » puissante est un atout essentiel dans la compétition mondiale et une composante importante de toute stratégie de puissance. Or l'Europe apparait de ce point de vue en net retrait par rapport aux Etats-Unis. Forte consommatrice de numérique, la faiblesse de son offre locale la conduit à exporter massivement ses données, principalement aux Etats-Unis. Comment passer d'une « Europe offerte » à une Europe « ouverte » ? Quelle est la situation des autres continents ? Peut-on parler de « géopolitique des données » ?

Axe 3 : les données, un capital menacé

Si les attaques en déni de service visent les infrastructures elles-mêmes, les données sont souvent l'objectif ultime des attaquants, qu'il s'agisse de cybercriminalité (vol d'information, crypto-locking…) ou d'espionnage. Quelles sont les dernières tendances observées ? Quels sont les modes opératoires des cybercriminels ? Comment calculer la valeur de ses données pour engager des poursuites ?

Axe 4 : droit et données

La donnée est une notion immatérielle qui soulève de nombreuses questions au plan juridique. Peut-on appliquer la notion de propriété à la donnée, notamment à la donnée personnelle ? Quel lien entre données et territoire ? Comment mettre en œuvre efficacement le droit à l'oubli aujourd'hui consacré dans certains pays ? Comment définir le vol de données au plan pénal ?

Axe 5 : quelles stratégies de sécurité des données pour l'entreprise ?

Pour les entreprises, la sécurité des données repose sur une approche globale impliquant : classification des données, évaluation des données, analyse de risques, définition et mise en œuvre d'une stratégie de sécurité. Le développement du cloud computing et l'externalisation croissante de l'IT soulèvent à cependant de nombreuses questions. Peut-on utiliser « en toute sécurité » un CRM ou un ERP dans le Cloud ? Quelles conséquences en termes de maîtrise des données ? Comment assurer les risques liés aux données ?

Axe 6 : quelles technologies pour sécuriser les données ?

Le responsable sécurité des systèmes d'information dispose aujourd'hui d'une vaste bibliothèque d'outils et de technologies lui permettant de sécuriser ses données, qu'il s'agisse d'outil de protection, de destruction sécurisée, de détection de fuites d'information ou d'investigation. La vitesse du progrès technologique et le « time to market » imposé par le marché aux éditeurs sont-elles compatibles avec les cycles d'adoption relativement lents des organisations ? Compte tenu de ce même « time to market », comment intégrer la sécurité de façon native (security by design) dans les applications à disposition des utilisateurs ?

Axe 7 : données et enjeux sectoriels

La transformation numérique et les données qui la nourrissent irriguent l'ensemble des secteurs économiques et des activités humaines. Les données sont ainsi au cœur de la « smart revolution » qui touche aussi bien l'individu dans sa vie quotidienne, la collectivité ou l'entreprise au travers des objets connectés et de « l'informatique omniprésente ». Quels sont les enjeux liés aux données dans la « ville intelligente », « l'usine du futur », le monde médical etc. ?

Axe 8 : enjeux sociétaux et éthiques liés aux données.

La transformation numérique, et la croissance exponentielle des données qu'elle génère, constituent à n'en pas douter des opportunités. Mais la rapidité de cette évolution et ses conséquences majeures sur l'Homme militent également pour une certaine prise de recul et un questionnement éthique et philosophique. Au plan individuel, que signifie désormais la notion de « vie privée » ? Est-il également possible de replacer l'utilisateur au cœur de cette transformation en lui permettant de se réapproprier « ses » données ? Faut-il enfin imaginer, sur le modèle de la loi bioéthique, une loi sur l'éthique numérique fixant un cadre pour l'exploitation des données à des fins prédictives ou à des fins de surveillance ?

Réagissez à cet article

Source : *Le FIC 2016 aura lieu les 25 et 26 janvier 2016 sur le thème de la sécurité des données | Observatoire FIC*

Les entreprises françaises bientôt condamnées à changer leur système de traitement des donnée personnelles ?

Les entreprises Françaises bientôt condamnées à modifier leur système de traitement des données personnelles ?

L’échéance se rapproche dangereusement. A partir de la fin du mois de janvier, entreprises américaines et européennes ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.

Le 6 octobre 2015, la Cour de justice européenne a en effet rendu une décision invalidant le « Safe Harbor », ce traité transatlantique sur le transfert des données personnelles. Premiers touchés, les géants américains du numérique, comme Facebook, Google ou Microsoft, qui exploitent massivement les donnes personnelles.

Qu’en est-il des entreprises françaises qui, sans toujours le savoir, communiquent les données personnelles de leurs clients. De leurs salariés, de leurs contacts… sur des serveurs aux États Unis ? (Gmail, DropBox, Google Drive…)

A partir de la fin du mois de janvier, les entreprises américaines et européennes, et donc françaises, ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.

Vous avez des doutes, vous souhaitez être accompagné ?
contactez-nous

Réagissez à cet article

Source : *Fin du « Safe Harbor » : Gattaz tire la sonnette d’alarme*