Les Français plus vulnérables aux virus propagés par clé USB

Les Français plus vulnérables aux virus propagés par clé USB

Les logiciels malveillants s'adaptent et les menaces en matière de cybersécurité varient d'un pays à l'autre, révèle une étude menée par la société de sécurité informatique Avira.

Vols de mots de passe, chevaux de Troie, ver, applications indésirables… En matière de cybersécurité, chaque pays «cultive» son défaut et son logiciel malveillant : tel est le principal enseignement d'une étude publiée lundi par la société de sécurité informatique Avira.
Le talon d'Achille de la France – l'un des cinq pays étudiés avec les Etats-Unis, le Royaume-Uni, l'Allemagne et l'Italie – se trouverait… dans la clé USB. Infestée de «vers».
Avira a en effet remarqué que le logiciel malveillant le plus fréquent en France était un ver, ou *worm* en anglais, de son nom technique Verecno.Gen. Son mode de contamination favori ? L'utilisation de clés USB. Celui-ci «n'est pas sans risque, rappelle la société dans son étude. Le ver Verecno est ainsi capable de se propager automatiquement dès que la clé USB est insérée dans l'appareil. Savez-vous d'où vient la clé USB qui vous est tendue ?» Avira délivre un conseil particulier aux Français : «Ne sur-socialisez pas».

A chaque pays son point faible

Les utilisateurs des Etats-Unis sont davantage vulnérables aux chevaux de Troie modifiant le comportement des systèmes d'exploitation Windows de leurs ordinateurs, les Allemands aux kits d'exploitation prospérant sur les défauts de mise à jour, les Italiens aux vols de mots de passe via les emails et les Britanniques au téléchargement d'applications indésirables.

leparisien.fr

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : les Français plus vulnérables aux virus propagés par clé USB – Le Parisien*

WhatsApp et Telegram corrigent des vulnérabilités importantes

WhatsApp et Telegram corrigent des vulnérabilités importantes

---

WhatsApp et Telegram ont corrigé des failles dans leurs applications après que des chercheurs en sécurité ont révélé qu'il était possible de prendre le contrôle des comptes d'utilisateurs.

WhatsApp et Telegram sont deux applications de messagerie instantanée qui ont plus d'un milliard d'utilisateurs cumulés. Elles offrent des communications chiffrées, un envoi de messages rapide et un tas d'autres fonctionnalités. Mais de nouvelles recherches révèlent qu'une image injectée par un logiciel malveillant aurait suffi à voler les comptes Web WhatsApp ou Telegram d'une personne. Il faudrait seulement quelques secondes pour que l'attaquant obtienne un contrôle total sur les comptes, y compris l'accès aux images, aux vidéos, aux fichiers audio et aux contacts. Et le cryptage serait effectivement une aide avec ce genre de hack.
La vulnérabilité était présente sur les versions desktop des applications, ainsi si vous n'utilisez pas WhatsApp ou Telegram sur votre ordinateur, alors vous étiez déjà à l'abri.
Les chercheurs en sécurité ont découvert que le code malveillant pouvait être caché à l'intérieur d'une image. Lorsqu'il est cliqué, le fichier image exécute le code et l'attaquant obtient un accès complet aux données de stockage WhatsApp et/ou Telegram. Le pirate pourrait ensuite envoyer le fichier à tous les contacts de la victime, en diffusant le malware à d'autres cibles.
Découverte par Check Point, la vulnérabilité a été communiquée à WhatsApp et Telegram le 8 mars, et les deux entreprises ont déjà déployé des correctifs pour leurs clients desktop…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *WhatsApp et Telegram corrigent des vulnérabilités importantes – Gridam*

Formations en cybersécurité en France

À titre indicatif, voici la liste des formations en cybersécurité délivrant un titre reconnu par l'État (ministère en charge de l'enseignement supérieur ou CNCP) de niveau équivalent à Bac+3 (licence professionnelle) jusqu'à Bac+5 (master, ingénieur).

Cette liste de formations a vocation à informer les étudiants sur l'ensemble des programmes accessibles. Ne figurent dans cette liste ni la formation continue, ni les titres non reconnus officiellement par l'État (DU, masters spécialisés, BADGE, etc.).
Les éléments fournis ci-dessous sont issus d'une récolte de données multiples et éparses dans l'ensemble des établissements d'enseignement supérieur en France. Cette liste n'est plus maintenue et sera supprimée en juillet 2027.

En savoir plus sur SecNumedu, le label de formations initiales en cybersécurité de l'enseignement supérieur

FORMATIONS RECENSÉES DE NIVEAU LICENCE

NOM ETABLISSEMENT	NOM FORMATION	SITE INTERNET
Cnam Bretagne	Licence Pro « Analyste en Sécurité des Systèmes Télécoms Réseaux et Informatiques » ASSTRI	http://cnamsecuritedefense.fr/formation-securite-telecoms-reseaux/
Université d'Aix-Marseille	Licence Pro « Administration et sécurité des réseaux d'entreprises »	http://iut.univ-amu.fr/diplomes/licence-professionnelle-reseaux-telecommunications-specialite-administration-securite
Université d'Artois	Licence Pro « Systèmes informatiques et logiciel – Sécurité informatique »	http://formations.univ-artois.fr/cdm33rc2/ws7_cmd=getFormation&_oid=FR_RNE_0623957F_FR_L3LSEIN291&_redirect=voir_fiche_programS_lang=fr-FR&_onglet=Description
Université de Clermont-Ferrrand 1	Licence Pro « Administration et Sécurité des Réseaux »	http://iutweb.u-clermont1.fr/xfTest?xml/formation?idFormation=16824
Université de Grenoble Joseph Fourier	Licence Pro « Réseaux Sans Fil et Sécurité »	https://iut1.ujf-grenoble.fr/formation-et-metier/licence-professionnelle/reseaux-et-telecommunications
Université de Grenoble Pierre Mendès France	Licence Pro « Administration et Sécurité des réseaux »	http://www.iut-valence.fr/licence-professionnelle-asur
Université de Haute-Alsace	Licence Pro « Administration et Sécurité des réseaux »	http://www.iutcolmar.uha.fr/fr/LP-RT-ASUR-260.html
Université de la Réunion	Licence Pro « Réseaux Sans Fil et Sécurité »	http://www.iut-lareunion.fr/licences/reseaux-a-telecommunications
Université de la Rochelle	Licence Pro « Administration et sécurité des réseaux »	http://www.iut-larochelle.fr/licences-professionnelles/lp-administration-et-securite-des-reseaux
Université de Valenciennes et du Hainaut Cambrésis	Licence Pro « Collaborateur de Défense et Anti Intrusion des Systèmes Informatiques (CDAISI) »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-5899
Université de Montpellier 2	Licence Pro « Administration et sécurité des réseaux »	http://www.iutbeziers.univ-montp2.fr/licence-pro-reseaux-et-telecoms.html
Université de Lorraine	Licence Pro « Réseaux Sans Fil et Sécurité »	http://iutnb.univ-lorraine.fr/index.php?op=lbaccplus3/lp_rt_reseaux.htm
Université de Nantes	Licence Pro « Administration et sécurité des réseaux »	http://www.iutlaroche.univ-nantes.fr/70407600/0/fiche___formation/&RH=IUTRY_FR1
Université Paris Est Créteil Val de Marne	Licence Pro « Réseaux informatiques, mobilité, sécurité (R3MS) »	http://www.u-pec.fr/pratiques/universite/formation/licence-professionnelle-reseaux-informatiques-mobilite-securite-rims-641083.kjsp
Université Paris 13	Licence Pro « Administration et Sécurité en Réseaux »	http://www.iutv.univ-paris13.fr/formations/licences-pro/reseaux-et-telecommunications.html
Université de Paris Sud	Licence Pro « Sécurité des Réseaux et Systèmes informatiques »	http://www.iut-orsay.u-psud.fr/fr/formations/licences_professionnelles/info_lp_srsi.html
Université de Rennes 1	Licence Pro « Administration et Sécurité des Réseaux »	http://sfc.univ-rennes1.fr/informatique/lp_administration-securite-reseaux.html#.U-R2OVRX6lB
Université de Rouen	Licence Pro « Administration Sécurité des Réseaux »	http://iutrouen.univ-rouen.fr/licence-professionnelle-administration-et-securite-des-reseaux-279942.kjsp
Université de Toulouse 2	Licence Pro « Réseaux Sans Fil et Sécurité »	http://www.univ-tlse2.fr/accueil/formation-insertion/decouvrir-nos-formations/licence-professionnelle-reseaux-sans-fil-et-securite-885.kjsp
Université de Tours	Licence Pro « Qualité – Sécurité des Systèmes d'Information »	http://iut-blois.univ-tours.fr/formations/qualite-securite-des-systemes-d-information-92850.kjsp
Université de Versailles Saint-Quentin	Licence Pro « Administration et Sécurité des Réseaux »	http://www.uvsq.fr/licence-professionnelle-metiers-des-reseaux-informatiques-et-telecommunications-parcours-administration-et-securite-des-reseaux-341092.kjsp?RH=1271771445917
Université de Pau et des Pays de l'Adour	Licence Pro « Administration et Sécurité des Réseaux »	http://iutpa.univ-pau.fr/live/RT/LP/LP+ASUR
Université de Bordeaux 1	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-bordeaux.fr/formations/programme.jsp?f=0&t=3000&p=2213
Université des Antilles et de la Guyane	Licence Pro « Administration et Sécurité des Réseaux »	http://sut.univ-ag.fr/formations/licences-professionnelles/lp-asur/

FORMATIONS RECENSÉES DE NIVEAU MASTER

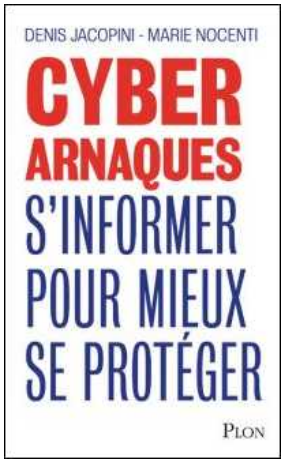
NOM ETABLISSEMENT	NOM FORMATION	SITE INTERNET
Université de Basse Normandie	Master « Réseaux et sécurité des systèmes informatiques »	http://www.unicaen.fr/formations/formations-proposees/master-pro-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-388756.kjsp
Université de Bordeaux 1	Master « Cryptologie et sécurité informatique »	http://www.math.u-bordeaux1.fr/~gzemor/dossier_CSI/
Université de Bretagne Sud (ENSIBS)	Ingénieur « Management et Ingénierie de sécurité des systèmes – cyberdéfense »	http://www-ensibs.univ-ubs.fr/devenir-ingenieur-en-cyberdefense-debouches-356662.kjsp?RH=1351525595668&RF=1351525595668
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cryptologie, sécurité et codage de l'information »	http://www-fourier.ujf-grenoble.fr/enseignement/spip.php?rubrique19
Université Grenoble Alpes	Master « Sécurité, audit, informatique légale – SAFE »	http://www.ujf-grenoble.fr/formation/diplomes/masters/domaine-sciences-technologies-sante/master-mention-mathematiques-informatique-specialite-securite-audit-informatique-legale-safe-p-838102.htm
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cybersecurité »	http://cybersecurity.imag.fr/
Université de Limoges	Master « Sécurité de l'Information et Cryptologie – CRYPTIS »	http://www.cryptis.fr/
Université de Lorraine (Mines Nancy, Telecom Nancy, ENSEM)	Master « Security of Computer Systems »	http://www.mines-nancy.univ-lorraine.fr/content/master-science-msc-security-computer-systems
Université de Lorraine	Master « Services, sécurité des systèmes et des réseaux »	http://msm.univ-lorraine.fr/content/master-informatique-ssr
Université de Lorraine	Master « Sécurité des systèmes d'information et de communication – SSIC »	https://formations.univ-lorraine.fr/fr-FR/fiche/presentation/UL-PROG2654/UL-PROG3211
Université de Lyon 1	Master SAFIR, parcours « Sécurité des systèmes informatiques en finance et en assurance – S2IFA »	http://isfa.univ-lyon1.fr/parcours_S2IFA
Université de Lyon 2	Master « Organisation et protection des systèmes et des réseaux – OPSIE »	http://www.univ-lyon2.fr/master-informatique-specialite-informatique-decisionnelle-et-statistique-opsie-264018.kjsp
Université de Nice Sophia Antipolis	Ingénieur « CryptograAphie, Sécurité, et vie Privée dans les Applications et Réseaux »	http://www.polytechnice.fr/informatique/page251.html
Université de Paris 8, en partenariat avec Paris Diderot (Paris 7)	Master « Mathématiques fondamentales et protection de l'information »	https://www.univ-paris8.fr/Master-Mathematiques-pour-la-protection-de-l-information
Université de Paris-Diderot (Paris 7) — en partenariat avec Paris 8	Master « Mathématiques, Informatique et applications à la Cryptologie – MIC »	http://www.math.univ-paris-diderot.fr/formations/masters/mic/index
Université de Paris-Est Créteil (Paris 12)	Master « Sécurité des systèmes informatiques »	http://www.lacl.fr/ens/master.html
Université de Poitiers	Master « Management des risques informationnels et industriels »	http://irisaf.univ-poitiers.fr/formation/master-management-des-risques-des-systemes-d-information/master-professionnel-et-recherche-sciences-technologies-sante-mention-gestion-des-risques-specialite-management-des-risques-des-systemes-d-information-11079.kjsp
Université de Reims Champagne-Ardenne	Master spécialité informatique, parcours « Administration et sécurité des réseaux »	http://www.master-informatique.net
Université de Rennes 1	Master « Sécurité des Systèmes d'Information – ISTIC »	http://etudes.univ-rennes1.fr/masterInformatique/themes/SecondeAnnee/Specialites/SSI
Université de Rennes 1, Université de Bretagne Sud, Université de Bretagne Occidentale, ENS Rennes, ENIB, ENSTA Bretagne, INSA Rennes, CentraleSupélec, Télécom Bretagne	Master « Sécurité des contenus et des infrastructures informatiques »	http://master.irisa.fr/index.php/fr/parcoursprog-fr/parcours-rennes-3-fr
Université de Rouen	Master « Sécurité des Systèmes Informatiques (SSI) »	https://dpt-info-sciences.univ-rouen.fr/index.php/accueil-mssi
Université de Valenciennes	Master « Informatique, réseaux et sécurité – IRS »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-7415
Université de Versailles-Saint-Quentin	Master « Sécurité des contenus, des réseaux, des télécommunications et des systèmes – SeCReTS »	http://www.master-secrets.uvsq.fr/
Université d'Orléans	Master « Informatique Nomade, intelligence et sécurité »	http://formation.univ-orleans.fr/fr/formation/offre-de-formation/master-lmd-XR/sciences-technologies-sante-STS/master-informatique-specialite-informatique-nomade-intelligence-et-securite-finalite-professionnelle-et-recherche-program-sciesf2-502-2.html
Université du Havre	Master « Systèmes informatiques, Réseaux et Sécurité – MATIS »	http://matis.univ-lehavre.fr/
Université Pierre et Marie Curie (Paris 6) — avec l'AFTI	Master « Informatique, spécialité SFPN, filière sécurité informatique — MSI »	http://www-master.ufr-info-p6.jussieu.fr/lmd/specialite/sfpn/
Université Technologique de Troyes	Master « Sécurité des systèmes d'information »	http://www.utt.fr/fr/formation/master-en-sciences—technologies—sante/specialite-ssi.html
Université de Valenciennes et du Hainaut-Cambrésis	Master « Cyber-défense et sécurité de l'information – CDSI »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-15674
ENSICAEN	Ingénieur « Monétique et sécurité des systèmes »	https://www.ensicaen.fr/formations/masteres-specialises-cpa/masteres-monetique-et-transactions-securisees/
EPITA	Ingénieur « Systèmes, réseaux et sécurité – SRS »	http://srs.epita.fr/
EPSI	Programme Ingénierie informatique – option Sécurité Informatique	http://www.epsi.fr/Programmes/Programme-Ingenierie/Ingenierie-5eme-annee
ESAIP	Ingénieur « Informatique et réseaux, spécialité cybersécurité »	http://www.esaip.org/formations/ingenieur-informatique
ESGI	Mastère « Sécurité informatique »	http://www.esgi.fr/master-informatique/master-securite-informatique.html
ESIEA	Ingénieur parcours « Fondamentals of Security (SEC) »	http://www.esiea.fr/formation-ingenieurs/majeures-ecole-ingenieurs/
ESIGELEC	Ingénieur « Architecture et sécurité des réseaux – ASR »	http://www.esigelec.fr/fr/dominantes
ETNA-Alternance	Ingénieur « Architecte système réseaux et sécurité »	http://www.etna-alternance.net/formation-2e-annee.aspx
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	http://www.eurecom.fr/fr/les-formations/ingenieur-de-specialisation/securite-des-systemes-informatiques-et-des-communications
IIA Laval	Manager en ingénierie informatique (M2I) option « Management de la sécurité des systèmes d'information (MSSI) »	http://iia-laval.fr/ecole-superieure-en-informatique/l3m1m2-diplome-m2i/bac5-diplome-m2i/
INSA Centre Val de Loire	Ingénieur « Sécurité et technologies informatiques »	http://www.insa-centrevaldeloire.fr/formation/securite-et-technologies-informatique
IONIS-STM	Master « Ingénierie informatique & Management : Sécurité informatique »	http://ionis-stm.com/master-securite-informatique.aspx
ISIMA-Université Blaise Pascal	Ingénieur « Réseaux et Sécurité Informatique »	http://www.isima.fr/f5-reseaux-et-securite/
Supélec (Rennes)	Ingénieur « Systèmes d'information sécurisés »	http://www.rennes.supelec.fr/ren/fi/sis/
Télécom Lille	Ingénieur « Sécurité des réseaux et des systèmes »	http://www.telecom-lille.fr/specialisations-sciences-et-technologies
Télécom SudParis	Ingénieur « Sécurité des systèmes et des réseaux »	http://www.telecom-sudparis.eu/p_fr_formations-post-grade_MS_1178.html?idm=65
Toulouse Ingénierie	Ingénieur « TLS-SEC »	http://tls-sec.github.io/tls-sec/

À voir aussi

- Formations labellisées SecNumedu
- Profils métiers de la cybersécurité
(Lien ne mène)

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *Formation et cybersécurité en France | Agence nationale de la sécurité des systèmes d'information*

Le cyber-espionnage, en tête

des menaces en 2017 ?

	**Le cyber-espionnage, en tête des menaces en 2017 ?**

Selon Trend Micro, l'augmentation des ransomware et des attaques menées par des Etats constituent un risque croissant pour les infrastructures critiques.

La dernière étude menée par Trend Micro, soutient que 20 % des entreprises mondiales classent le cyber-espionnage comme la plus forte menace pour leur activité, 26 % luttant pour suivre et anticiper l'évolution rapide des différentes menaces. Aux Etats-Unis, 20 % ont déjà subi une attaque de ce type en 2016.
L'étude révèle que le cyber-espionnage arrive en tête des préoccupations de sécurité pour 2017, suivi par les attaques ciblées (17 %) et le phishing (16 %). Les entreprises situées en Italie (36 %), en France (24 %), en Allemagne (20 %) et aux Pays-Bas (17 %) sont celles qui craignent le plus le cyber-espionnage, ce qui s'explique notamment par la tenue d'élections dans chacun de ces pays cette année.
Huit pays sur dix ont mentionné le caractère de plus en plus imprévisible des cybercriminels (36 %) comme étant le plus grand frein à la protection contre les cyber-menaces. Ils sont également 29 % à faire état de lacunes concernant la compréhension des dernières menaces, et 26 % à s'efforcer de suivre l'évolution rapide des menaces et la sophistication croissante des activités cybercriminelles.
Selon l'étude, près des deux tiers (64 %) des entreprises avaient subi une cyber-attaque majeure « connue » au cours des 12 derniers mois. En moyenne, elles en avaient même connu quatre. Les menaces de type ransomware étaient de loin les plus courantes, 69 % des personnes interrogées indiquant avoir été attaquées au moins une fois au cours de la période. En réalité, seul un quart (27 %) des entreprises interrogées n'avait pas été ciblé par un ransomware.

Autre fait notable : à peine 10 % des entreprises pensent que les attaques de type ransomware constitueront une menace en 2017, alors que l'année 2016 a été marquée par une augmentation de 748 % de ces attaques, avec 1 milliard de dollars de pertes pour les entreprises à travers le monde. On estime que le nombre de ransomware va augmenter d'encore 25 % en 2017, s'attaquant à divers appareils tels que les téléphones portables, les objets connectés (IoT) et les dispositifs d'IoT industriel (IIoT)…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Le cyber-espionnage, en tête des menaces en 2017* |

Google, ou la révolution transhumaniste via le Big Data

Google, ou la révolution transhumaniste via le Big Data

A l'occasion de la sortie du livre de Christine Kerdellant Dans la Google du loup, Éric Delbecque décrypte le projet de « fusion » entre le vivant et le digital porté par le géant de l'informatique américain.

Christine Kerdellant a relevé un beau défi *Dans la Google du loup* (Plon)! Elle met le doigt là où Google pose véritablement problème, à savoir sur la révolution anthropologique du transhumanisme… Pour ce qui concerne sa participation à la société de surveillance globale que fabriquent un certain nombre d'acteurs publics et privés, l'affaire est entendue depuis des années… Sous l'administration Obama, les dirigeants de Google se rendirent à la Maison-Blanche 230 fois! Ils confirmèrent en 2013 que les agences gouvernementales de l'Oncle Sam les sollicitaient annuellement – dans le cadre du Patriot Act – pour surveiller 1000 à 2000 comptes. En janvier 2015, la firme vedette du Web a reconnu avoir fourni au Ministère de la Justice américain l'intégralité des comptes Google de trois membres de WikiLeaks.

Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons.

Il paraît dès lors compliqué de penser qu'une idéologie sécuritaire explique à elle seule l'extension de l'ombre de Big Brother sur le monde. Les géants du numérique du secteur privé (les GAFA: Google, Amazon, Facebook, Apple) participent largement à la manœuvre, plus ou moins volontairement (pas pour des raisons politiques, mais économiques). Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons. Sa stratégie en matière de renseignement doit se lire comme un fragment d'un système cybernétique (au sens de science du contrôle) beaucoup plus vaste, où le capitalisme financier californien et numérique occupe une place décisive. Séparer ce dernier du complexe militaro-sécuritaro-industriel de l'Oncle Sam devient de plus en plus difficile, voire hasardeux.

L'intérêt plus décisif du livre de Christine Kerdellant est ailleurs. Il explore de manière très accessible et percutante le cœur du projet Google, ou plutôt sa signification philosophique profonde. Derrière les joyeux Geeks de la Silicon Valley s'exprime la volonté de réifier l'humanité, de l'enchaîner à une raison calculante. Cette dernière va nous émanciper nous répète-t-on, nous libérer – via le Big Data – des limites de notre condition, nous délivrer de la mort et transformer notre existence en un jardin de fleurs. Mais lorsqu'on choisit d'examiner de plus près les conséquences des propositions de Google, on découvre une perspective d'avenir moins réjouissante…[lire la suite]

Réagissez à cet article

Source : *Google, ou la révolution transhumaniste via le Big*

Data

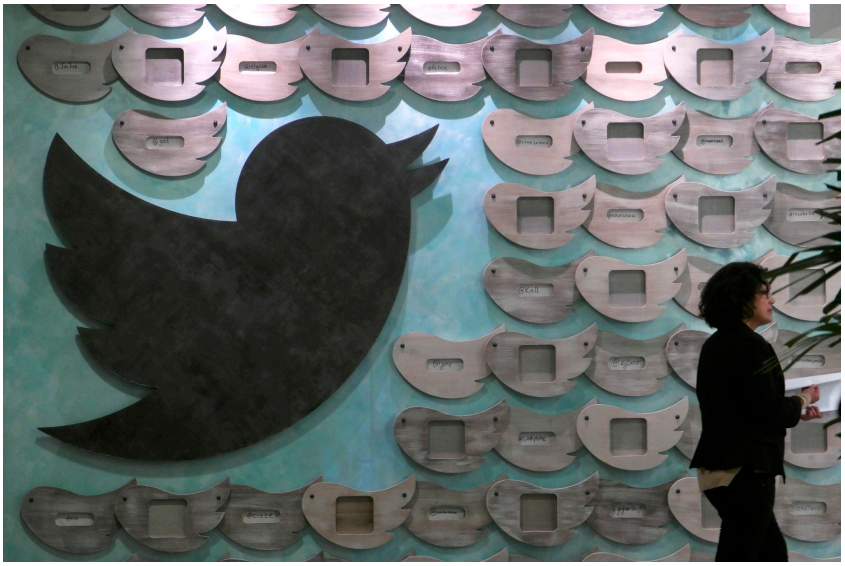
Le Bourget : ces drones vont vous faciliter la vie

De drôles d'engins vrombissaient ce mardi au Musée de l'Air et de l'Espace du Bourget.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur sur cette page.

Réagissez à cet article

La lutte du cyberharcèlement sur Twitter grâce à l'intelligence artificielle



La lutte du cyberharcèlement sur Twitter grâce à l'intelligence artificielle

Le réseau social va s'aider d'outils d'apprentissage automatique pour repérer plus vite les messages allant à l'encontre de ses règles d'utilisation

Un concert d'excuses et quelques mesures concrètes. Après plusieurs années de silence et d'hésitation, Twitter promet que 2017 sera l'année de la lutte contre le harcèlement. Le réseau social présente trois nouveaux outils pour limiter l'influence des discours de haine et des attaques ciblés contre ses utilisateurs. Ils seront déployés à partir de mardi. D'autres fonctionnalités devraient être présentées dans le courant de l'année. «Nous avons entendu vos critiques. Nous n'avons pas progressé assez l'année dernière», avait déclaré Ed Ho, vice-président de Twitter, fin janvier. «Nous continuerons à être attentifs à vos retours, d'apprendre des critiques et de sortir des nouvelles fonctionnalités jusqu'à ce que tous nos utilisateurs ressentent ces changements.» Twitter va se reposer sur une nouvelle arme pour l'aider dans sa modération: l'intelligence artificielle.

Repérer plus rapidement les agressions

Le nouveau plan de Twitter comporte trois mesures phares. La première doit lutter contre la création abusive de nouveaux comptes par des utilisateurs déjà bannis du réseau social. Il est difficile de repérer ces internautes. Il changent généralement d'adresse mail, de numéro de téléphone et d'adresses IP pour s'inscrire à nouveau. Twitter va s'appuyer sur un programme d'apprentissage automatique afin de repérer les resquilleurs. Tout compte banni définitivement du réseau social sera analysé afin de repérer des signaux permettant d'identifier une personne, comme une manière de parler, des sujets ou des victimes de prédilection, des hashtags préférés, etc. Si un nouveau compte Twitter correspond à cette analyse, il pourra être rapidement supprimé.

Twitter crée également une nouvelle option pour masquer les images choquantes dans les recherches de tweets. Sont concernées les photos pornographiques ou violentes. Elles seront repérées automatiquement. Par exemple, une personne tapant «Bataclan» dans la barre de recherche de Twitter devrait en théorie ne pas voir de photos de la tuerie. Cet outil devrait aussi être utile pour les personnes faisant l'objet d'une campagne de dénigrement, afin de ne pas voir son pseudo associé à des images pornographiques ou violentes. L'option sera enclenchée par défaut, mais pourra être désactivée dans les réglages Twitter.

Dernier outil lancé par le réseau social: les réponses à un tweet seront bientôt classées par ordre d'intérêt. Les messages automatiquement détectés comme «peu intéressants» par Twitter seront relégués en bas. Parmi les critères examinés par le réseau social: si le compte est nouveau et ne suit aucune autre personne, s'il a déjà été signalé pour abus ou qu'il emploie des insultes.

Accélérer le signalement

L'intelligence artificielle ne va pas remplacer les modérateurs de Twitter. Elle interviendra pour accélérer le signalement de contenus. Comme les autres réseaux sociaux, Twitter applique une modération *a posteriori*: les utilisateurs doivent lui signaler les contenus problématiques pour qu'ils soient contrôlés et éventuellement supprimés s'ils enfreignent les règles d'utilisation. Le réseau social collabore aussi avec les autorités qui peuvent lui signaler des contenus illégaux. En France, plus de 466 tweets ont fait l'objet d'une demande de retrait par la police ou le gouvernement entre janvier et juin 2016…[lire la suite]

Réagissez à cet article

Source : *Twitter s’appuie sur l’intelligence artificielle pour lutter contre le harcèlement*

Les dangers des jouets connectés | Denis JACOPINI

Les dangers des jouets connectés | Denis JACOPINI

La gamme Cloudpets de Spiral Toys a été piratée. Plus de 800000 comptes ont été piratés avec les informations qui y sont liées et plus de 2,2 millions de messages vocaux se retrouvent également sur la toile. Les peluches connectées de la marque permettait en effet aux parents et aux enfants de s'échanger des messages par le biais d'une application téléphonique, à travers l'ours en peluche.

Denis JACOPINI a été Interviewé par la revue Atlantico à ce sujet :

Atlantico : Une société d'ours en peluche connectés a été récemment piratée, les messages laissés par les parents à leurs enfants sont désormais hackable. Ce n'est pas la première fois que ce type de piratage arrive, pour protéger nos enfants, devrions-nous les éloigner de ce type de jouets connectés ?
Denis JACOPINI : En effet, au-delà du risque relatif à la protection des données personnelles des enfants et de leurs parents, la revue Que choisir avait déjà alerté les consommateurs en fin 2016 sur des risques inhérents au connexions non sécurisée de plusieurs jouets connectés.
Qui a tenu compte du résultat de cette étude pour revoir la liste des jouets qui seraient présents dans la hotte légendaire ?
La relation entre les enfants et les jouets va bien au-delà de la technologie et des risques qu'elle peut représente.
Les jouets bénéficie également de phénomènes de mode et l'engouement, sauf erreur, se fout bien de la qualité des produits et encore moins de leur sécurité.
Manque de connaissance, inconscience, crédulité ou trop de confiance de la part des parents ? Il est vrai qu'on peut facilement croire que si des jouets se trouvent sur nos rayons, c'est qu'ils ont forcément dû passer avec succès toute une batterie de tests rassurant pour le consommateur.
Pour la part des jouets à usage familial testés, même si les normes EN71 et EN62115 ont été récemment révisées pour répondre aux exigences de la nouvelle directive 2009/48/CE, les validations se reposeront sur des niveaux satisfaisants en terme de propriétés physiques et mécaniques, d'inflammabilité, de propriétés chimiques, électriques ou bien relatives à l'hygiène et à la radioactivité.
Vous l'aurez remarqué, aucun test n'est prévu pour répondre à des mesures ne serait-ce que préventive en terme de protection des données personnelles et encore moins en matière se sécurité numérique.
Alors finalement, pour répondre à votre question : « devrions-nous éloigner les enfants de ce type de jouets connectés ? »
A mon avis, en l'absence de normes protectrices existantes, la prudence devrait être de mise. Certes, il est impossible de se protéger de tout. Cependant, il serait à minima essentiel que les parents soient informés des risques existants et des conséquences possibles que pourraient provoquer des piratages par des personnes mal intentionnées pour prendre des mesures qu'ils jugent utiles.

Atlantico : Comment pouvons-nous restreindre la possibilité de piratage de données pour ce type d'objet ?
D.J. : La situation confortable serait que le consommateur soit vigilant pour ce qui concerne les mesures de sécurité couvertes par l'appareil et celles qui ne le sont pas. Malheureusement, ces gardes-fous ne sont qu'à l'état d'étude.
Sauf à vous retrouver dans un environnement ou le voisin le plus proche se trouve à plusieurs dizaines de mètres, être prudent dans l'usage de ces objets pourrait par exemple consister à :
– Si le jouet le permet, changer le mot de passe par défaut et mettre en place un mot de passe complexe pour accéder à sa configuration ;
– Si le jouet le permet, activer les connexions sécurisées par cryptage ;
– Si le jouet le permet, désactiver les connexions à partir d'une certaine heure ;
– N'utiliser les jouets connectés que dans des environnements protégés, en raison de la portée limitée des communications Bluetooth (par des distances suffisantes entre le jouet et des pirates éventuels) ;
– Pour les jouets utilisant le Wifi,
– Mettre en place des protections physiques contre les rayonnements électromagnétiques dans certaines directions ;
– Cacher les caméras si elles ne sont pas utilisées ;
– En fin d'utilisation du jouet, ne pas se satisfaire d'éteindre l'appareil qui ne sera peut-être seulement en veille, mais retirer les piles ou placer le jouet dans un espace protégé (fabriquez une cage de Faraday) ;
Enfin, compte tenu que le bon fonctionnement du jouet est lié à l'acceptation des conditions contractuelles d'utilisation des donnés personnelles ne respectent pas les règles européennes relative à la protection de ces données et de la vie privée car les fabricants sont généralement situés hors Europe, ne pas accepter ces conditions reviendrait à être privé de l'usage des fonctions du jouet.

Atlantico : Concrètement, les objets connectés sont une porte ouverte à notre intimité, quels sont les dangers liés à ce type d'objets ?
A défaut d'information de la part des fabricants et d'alerte de la part des médias, il serait, à mon avis, adapté que le consommateur reconsidère les objets numériques et particulièrement les objets connectés comme étant des équipements dont les fonctions et conséquences induites risquent de se retourner contre son utilisateur.
L'année dernière, l'association de consommateurs UFC-Que choisir a mis en garde les consommateurs sur le stockage des données. Elle a d'ailleurs saisi sur le sujet la Commission nationale de l'informatique et des libertés et la Direction générale de la concurrence, de la consommation et de la répression des fraudes.
En effet, tout ce que disent les enfants à la poupée testée est enregistré et mystérieusement stocké sur des serveurs à l'étranger et géré par la société Nuance Communications. L'Association européenne de défense des consommateurs a déclaré : « Tout ce que l'enfant raconte à sa poupée est transmis à l'entreprise, basée aux États-Unis, Nuance Communications, spécialisée dans la technologie de reconnaissance vocale ».
Quelles sont les conséquences d'un tel usage de nos données ?
L'objectif évident est le matraquage publicitaire des enfants, car certains jouets ont une certaine tendance à faire souvent allusion à l'univers de Disney ou à Nickelodeon par exemple.
Enfin, des tests ont montré qu'un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom Bluetooth par défaut du jouet connecté, permet très simplement de les identifier.
Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.
Que ça soit en en terme d'écoute et d'espionnage à distance de l'environnement de l'enfant et de celui des parents, ou en terme de prise de contrôle à distance de l'appareil risquant de terroriser ou pire, traumatiser l'enfant, la prudence doit d'abord rester de mise.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Jouet connecté : après un piratage, les données de 800000 familles fuitent sur le web*

Les drones volent au secours des agriculteurs

Les drones volent au secours des agriculteurs

Et si l'avenir de l'agriculture se jouait… dans les airs ? Depuis quelques années, les exploitants agricoles ont effet la possibilité d'analyser leurs parcelles à l'aide d'un drone.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

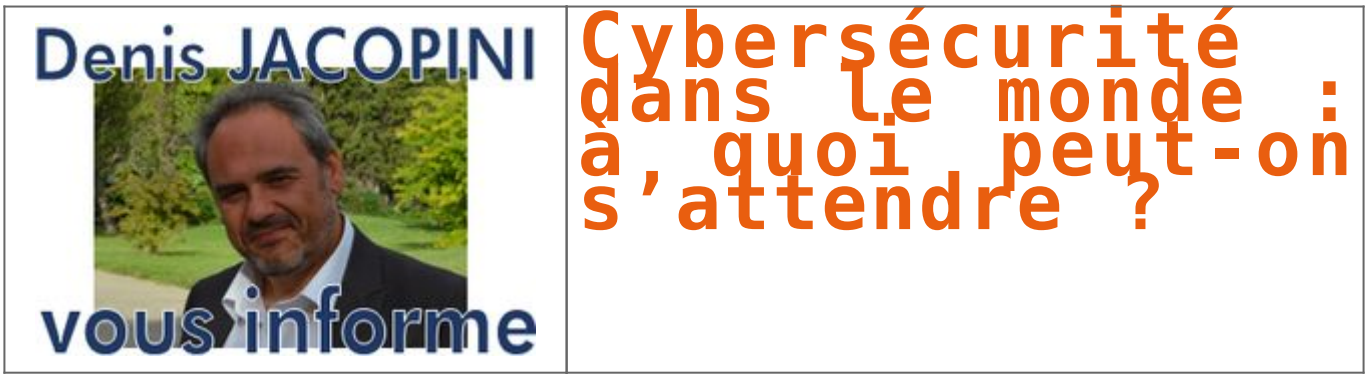
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Cybersécurité dans le monde : à quoi peut-on s'attendre ?



L'année 2016 a démontré que les mesures de sécurité traditionnelles ne suffisaient plus et que de nouvelles stratégies devaient être mises en place. 2017 va donc s'inscrire dans la continuité de ce qui a déjà été amorcé l'année passée, à savoir : toujours plus de sécurité pour toujours une protection maximisée. Les experts de NTT Security ont fait ressortir les tendances et les prévisions pour cette année qui débute.

Selon Garry Sidaway, Vice-Président Senior de la Stratégie de Sécurité

1. L'identité restera au cœur des enjeux

Au risque de nous répéter, les mots de passe fournissent aujourd'hui des garanties insuffisantes. À l'ère du digital et de la mobilité, commodité et sécurité ne font pas bon ménage. Certes, les mots de passe sont bien pratiques, mais ils sont de moins en moins perçus comme une preuve d'identité irréfutable. Devant l'utilisation croissante des smartphones et les exigences de simplicité des consommateurs et des professionnels, les solutions d'identité resteront donc au cœur des préoccupations en 2017. C'est ainsi que le mot de passe traditionnel cèdera du terrain face à la poussée du « multi-facteurs », une méthode combinant plusieurs facteurs d'authentification (localisation, possession d'un objet, d'une information, etc.). Cette association entre physique et digital, avec en toile de fond l'émergence de méthodes d'authentification avancées, favorisera le développement de nouvelles solutions de gestion des identités.

2. Le mobile sera omniprésent

Au royaume du digital, le mobile est roi. Un roi qui bouscule l'ordre établi dans de nombreux domaines, des méthodes de paiement jusqu'aux interactions sociales. Véritables hubs digitaux, nos smartphones constituent désormais non seulement une fenêtre de contrôle et d'interaction avec le monde mais aussi une interface d'identification et d'authentification. Dans un tel contexte, 2017 verra le curseur de la menace se déplacer des ordinateurs portables vers les appareils mobiles. Si, traditionnellement, les acteurs de la sécurité se sont concentrés sur les systèmes back-end et les conteneurs, ils devront revoir leur approche pour placer le mobile au cœur de leur dispositif.

3. Les entreprises surveilleront la menace interne

Le problème des menaces internes ne date pas d'hier. Côté défense, les progrès réalisés dans les domaines de l'analytique et de la détection des anomalies devraient se poursuivre en 2017. Dans un milieu de l'entreprise de plus en plus dynamique, définir les critères d'un comportement utilisateur « normal » restera un défi de taille. Toutefois, avec le développement de nouvelles techniques de machine learning, nous verrons l'analyse comportementale s'opérer directement au niveau des terminaux.

4. Fin de la détection basée sur les signatures

Antivirus nouvelle génération, solutions de sécurité des terminaux, solutions de détection et de réponse aux incidents… Peu importe leur nom, les solutions de protection des terminaux se projetteront bien au-delà de la détection basée sur des signatures statiques, à commencer par les outils d'analyses avancées que l'on retrouvera systématiquement sur ces solutions. Leur force résidera notamment dans leur capacité à exploiter la puissance du cloud pour partager l'information sur les menaces connues. La diversité et le volume sans précédent des malwares engendreront l'émergence d'une nouvelle approche. Destinée à enrayer le syndrome dit du « patient zéro », cette démarche reposera à la fois sur une collaboration internationale et l'utilisation d'une cyberveille prédictive et proactive pour libérer toute la force du collectif.

5. Le tout-en-un fera de plus en plus d'adeptes

Alors que le marché de la cybersécurité se consolide, les entreprises se tournent vers des solutions de sécurité couvrant l'intégralité des environnements TIC. Traditionnellement, la force des prestataires de sécurité managée (MSS) s'est située dans leur capacité à intégrer un maillage d'outils complexes et pointus. Aujourd'hui, la situation a changé. Tout l'enjeu consiste à intégrer le facteur sécurité à tous les échelons du cycle opérationnel de l'entreprise. Les clients chercheront donc un partenaire capable d'agir sur tous les fronts : applications métiers, infrastructure réseau, services cloud et de data center autour d'une console de gestion centralisée. En 2017, les solutions multifournisseurs apparaîtront comme datées. Les acteurs de la sécurité devront ainsi coordonner un service complet de bout en bout pour répondre aux enjeux de l'espace de travail digital.

Selon Stuart Reed, Directeur Senior Product Marketing

6. Les consommateurs exigeront plus de transparence

Une étude récente de NTT Security a mis en lumière les attentes croissantes des cyberconsommateurs en matière de transparence, tant sur le plan des pratiques que de la gestion des incidents. Ces conclusions traduisent notamment une sensibilisation accrue des consommateurs sur les questions de sécurité suite aux scandales de violations à répétition. La tendance est appelée à se poursuivre en 2017 et au-delà. Notons enfin que les entreprises dotées de politiques de sécurité et de plans d'intervention efficaces diminueront leur exposition au risque, tout en profitant d'un puissant levier de compétitivité.

7. L'innovation en moteur de consolidation

Du point de vue de l'offre comme des fournisseurs de cybersécurité, 2016 a été placée sous le signe de la consolidation. Au rang des plus grosses opérations, on citera l'acquisition de BlueCoat par Symantec, la série de rachats par Cisco et, plus proche de nous, la création de NTT Security autour de trois piliers : analytique de pointe, cyberveille avancée et conseils d'experts en sécurité. Derrière ce phénomène de consolidation, on retrouve une constante : l'innovation. Concrètement, les grandes entreprises ont racheté des spécialistes pour accéder à leurs compétences et les englober dans une offre plus aboutie. Ces grands acteurs profitent enfin d'économies d'échelle considérables – et de l'expertise et de l'efficacité qui en découlent – pour mener des programmes d'incubation qui viendront à leur tour stimuler l'innovation. Cette tendance de fond souligne bien l'importance de l'innovation pour évoluer au rythme des besoins de sécurité des clients.

8. L'identité des objets

Avec l'essor de l'IoT, la frontière entre physique et digital s'estompe peu à peu pour créer des expériences clients plus pratiques, rapides et efficaces. Seulement voilà, les cybercriminels ont eux aussi investi la sphère de l'IoT à l'affût de la moindre vulnérabilité. On a ainsi recensé des cyberattaques se servant d'objets connectés (caméras de vidéosurveillance, imprimantes…) pour lancer des attaques DDoS qui sont parvenues à paralyser des sites comme Twitter et Spotify. L'année 2017 verra sans doute une recrudescence des attaques perpétrées à l'encontre des objets connectés. D'où le besoin impérieux d'intégrer ces appareils à une politique de sécurité plus complète, notamment pour mieux contrôler l'identité et la légitimité de leurs utilisateurs.

9. L'analytique changera la donn

L'un des grands défis de la cybersécurité pourrait se résumer par cette question : comment produire une information cohérente à partir d'une avalanche de données issues de dispositifs multiples ? Si l'analyse de données a pour fonction première de « donner du sens », l'évolution des menaces doit nous inciter à revoir nos méthodes d'interprétation et de contextualisation de l'information. Dans cette optique, les outils avancés d'analyse du risque vous permettront de prendre les bonnes décisions. Au-delà des événements présents, ces outils ont pour fonction de décortiquer les données historiques pour faire ressortir des tendances, mais aussi d'utiliser l'intelligence artificielle pour identifier les schémas comportementaux annonciateurs d'une attaque. Fondées sur des technologies avancées de machine learning, des outils d'analyse automatiques et des experts en astreinte permanente, les solutions d'analytique de pointe promettent de changer la donne dans le secteur des MSS.

Selon Kai Grunwitz, Vice-Président Senior Europe Centrale

10. La cybersécurité va s'imposer comme un facteur clé de succès

Pour être reconnue comme tel par tous les acteurs concernés, la cybersécurité doit s'intégrer en amont à l'ensemble des processus métiers de l'entreprise. Dans un monde connecté où le digital gagne chaque jour en importance, les entreprises veulent pouvoir compter sur une sécurité parfaitement incorporée à leurs stratégies métiers et IT. Outre son rôle indispensable de gardienne des données sensibles, du capital intellectuel et des environnements de production, la cybersécurité sera également partie intégrante de l'innovation et de la transformation de l'entreprise.

La sécurité ne sera plus seulement le problème des DSI, mais s'invitera au cœur des processus métiers et constituera l'un des ressorts de la chaîne de valeur. Enfin, la gestion du cycle de sécurité constituera un différenciateur clé autant qu'une priorité essentielle dans le cadre d'une stratégie de sécurité orientée métiers. Elle procurera aux entreprises un avantage concurrentiel et un réel levier de valeur ajoutée.

Selon Chris Knowles, Directeur solutions

11. Le RGPD sera partout !

Si vous pensiez que le Règlement général sur la protection des données (RGPD) a été l'un des grands thèmes de 2016, attendez de voir ce que 2017 vous réserve. Alors que les fournisseurs proclameront les avantages de leurs technologies et que les équipes juridiques plancheront sur la définition d'une sécurité réellement irréprochable, les clients, eux, se lanceront dans les préparatifs.

12. Au royaume des aveugles, les borgnes sont rois… mais plus pour très longtemps !

Pour beaucoup d'entreprises, la sécurité se résume à la protection d'un périmètre au moyen de périphériques inline censés analyser l'intégralité du trafic et intervenir sur la base d'éléments visibles. Toutefois, la mobilité croissante des collaborateurs, associée à l'explosion du nombre d'applications cloud en entreprise, créent des « angles morts ». À commencer par le transit d'informations via des tunnels cryptés, le stockage et le traitement de données à l'extérieur de data centers sécurisés, ou encore les communications entre machines virtuelles qui échappent totalement à la surveillance des dispositifs de sécurité existants. En 2017, les entreprises se pencheront sur ce phénomène afin d'éliminer les angles morts et de reprendre le contrôle de leur sécurité.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Cybersécurité dans le monde : à quoi peut-on s’attendre ?*