Quelles tendances en 2017 pour la sécurité du Cloud ?

Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ». Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[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 : 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

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? – Globb Security FR

Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

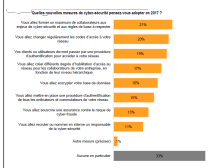
À l'exception des grands groupes, la majorité des entreprises françaises sous-estiment les risques de cyber-attaque ; moins de 4 sur 10 d'entre elles décideurs considèrent comme « important », ou « très important », le risque que leur société subisse une cyber-attaque ces prochaines années… et ce, alors que 52% des entreprises ont déjà été piratées. C'est ce que montre une enquête réalisée par le cabinet Denjean & Associés en partenariat avec Gan Assurances

Les décideurs d'entreprise se font de fausses idées sur la cyber-fraude. Plus de trois sur quatre sous-estiment la vitesse de propagation de ce fléau dans l'Hexagone, pensant que le nombre des cyber-fraudes recensées en France n'a augmenté « que » de 10% ou de 25% en 2015, alors qu'il a crû de 50% ! (Source : Anssi, Agence nationale de sécurité des systèmes d'information). Questionnés sur les cibles visées en priorité par les pirates, 50% des décideurs citent les multinationales ; et pour 23% des répondants, les organismes publics constituent le premier choix des hackers. Seulement 20% des personnes interrogées connaissent la bonne réponse : les PME concentrent dans notre pays près de 80% des cyber-attaques (source : Syntec).

Globalement, 70% des entreprises s'estiment bien protégées contre la cyber-fraude. Une statistique qui recouvre des disparités : 100% des grands groupes affichent leur confiance dans leurs process de cybersécurité, tandis que 58% des TPE et environ 75% des PME et des ETI se jugent bien protégées.

Quelles bonnes pratiques ?

Les entreprises ayant adopté une politique de cybersécurité ont mis en place, en moyenne, trois bonnes pratiques. Les plus répandues sont le changement régulier par l'entreprise des codes d'accès à son réseau (mesure existant dans 56% des structures), et l'instauration en son sein d'une procédure d'authentification de tous les ordinateurs et commutateurs (53% des entreprises). La formation interne aux enjeux et aux précautions de base en matière de cybersécurité, et la création de différents degrés d'accès au réseau pour les collaborateurs selon leur niveau hiérarchique (respectivement pratiquées par 45% et 44% des sociétés) se disputent la troisième place sur le podium.
Deux entreprises sur trois comptent adopter en 2017 de nouvelles mesures pour lutter contre le piratage informatique qui se décomposent comme l'indique l'infographie ci-dessous.



90% des entreprises françaises sont disposées à investir chaque année pour se protéger efficacement contre la cyber-fraude, et 60% sont même prêtes à y consacrer un budget supérieur ou égal à 1% de leur chiffre d'affaires. Parmi les différentes catégories d'entreprises, les PME et les ETI se montrent les plus enclines à réaliser un effort financier conséquent : les trois-quarts d'entre elles acceptent de dépenser chaque année pour leur cybersécurité entre 1% et 2% de leur chiffre d'affaires.
Si l'on exclut les dirigeants de très petites structures, peu ou pas du tout concernés par ces sujets, les décideurs apparaissent bien conscients des nouveaux risques encourus par les entreprises, et décidés à les combattre. En effet, 66% des décisionnaires indiquent qu'ils se préoccuperont au cours des trois années à venir de lutter contre les « ransomwares » ; 70% disent qu'ils s'attacheront à sécuriser les données mises sur le cloud ; et 70% déclarent qu'ils veilleront à prévenir les risques liés aux objets connectés…

Original de l'article mis en page : Les entreprises françaises sous-estiment les risques de cyber-attaque

---

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 : 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 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

100 000 emplois en Tunisie grâce aux smart-cities et objets connectés

100 000 emplois en Tunisie grâce aux smart-cities et objets connectés

La Tunisie se met au numérique pour son développement économique. Avec la régression de l'une des principales sources de revenu qu'est le tourisme, la Tunisie ambitionne d'optimiser son économie avec le projet « Tunisie Numérique 2020 ».
Le numérique, dans l'économie de la Tunisie, représente déjà 11% de taux de croissance annuelle et 7% du PIB, devant le secteur du tourisme. Avec les initiatives privées, le gouvernement travail à faire progresser ce chiffre.
« C'est la première fois que le secteur public se dit : « Je ne vais pas tout faire tout seul et il y a des secteurs que je connais mal », « De notre côté, nous sommes conscients qu'après la révolution, le rôle de la société civile devient plus important et c'est pourquoi nous mettons notre savoir-faire au service de la Tunisie », a expliqué l'entrepreneur, éditeur du logiciel Badredine Ouali, qui préside également le partenariat public-privé Smile Tunisia.
D'ici 2020, le gouvernement tunisien vise créer 100 000 emplois en misant sur les smart-cities ou les objets connectés.

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 : 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

Original de l'article mis en page : Tunisie: 100 000 emplois grâce aux smart-cities et objets connectés | Africa Top Success

Tendances actuelles et émergentes pour la cybersécurité en 2017

Tendances actuelles et émergentes pour la cybersécurité en 2017

Original de l’article mis en page : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 – Global Security Mag Online

---

Un raccourci Windows qui peut flinguer votre sécurité

Un raccourci Windows qui peut flinguer votre sécurité

Un chercheur Français découvre comment il est possible de télécharger et exécuter n'importe quel fichier en utilisant un outil natif de Windows. Une porte ouverte pour des infiltrations malveillantes.

Notre ami Jean-Pierre LESUEUR, le fondateur de Phrozen software n'est plus à présenter. Ce chercheur en sécurité informatique, auteur de nombreux logiciels permettant de contrer pirates et codes malveillants vient de trouver une petite finesse dans l'ensemble des Windows, et cela à partir du SP2 de Windows XP qui risque de faire réagir rapidement le géant américain. Le problème est simple, à travers un raccourci Windows, il est possible de télécharger et exécuter n'importe quel fichier en utilisant un outil natif de Windows. « ***Du coup forcement,*** explique Jean-Pierre Lesueur, ***indétectable par les Antivirus actuels car un raccourci n'est pas directement un fichier exécutable***« .

Seulement, cette première découverte a fait suite à une seconde 100 fois plus vicieuse encore. Réussir à injecter une application directement dans le raccourci, ainsi plus besoin de télécharger et exécuter le code malveillant. Bilan, les pare-feu ne risquent plus de bloquer la potentielle attaque. Bref, une nouvelle couche problématique…[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 : 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

Original de l'article mis en page : ZATAZ Quand un raccourci Windows peut flinguer votre sécurité – ZATAZ

Quels changements en Cybersecurité pour 2017 ?

Quels changements en Cybersecurité pour 2017 ?

Yahoo, Twitter, Spotify, Amazon, eBay, CNN… lannée 2016 aura été fructueuse en attaques informatiques majeures. Si, les conséquences sont limitées, elles prouvent que les hackers sont tenaces et créatifs. Faut-il sattendre à un nouveau type dattaque en 2017 ?

Historiquement, les cyber-pirates ont focalisé leur attention sur les grandes entreprises. Ces sociétés ont donc été les premières à adopter les nouvelles technologies, via des solutions souvent à peine testées. Résultat : elles peuvent plus facilement être compromises, via certaines failles qui n'ont pas encore été repérées par les fabricants. En conséquence, ce sont les grandes sociétés qui attirent les hackers en quête de nouveaux défis et subissent les attaques de grande ampleur.

En parallèle, par effet pyramidal, ces mêmes technologies sont progressivement adoptées par les moyennes entreprises puis, en bas de pyramide, par les PME. Lorsque le deuxième échelon de la pyramide est atteint, les technologies sont plus sécurisées grâce au retour d'expérience. Les hackers les délaissent donc bien souvent pour se concentrer sur des technologies plus récentes.

Mais 2017 devrait marquer un tournant : en effet, ce sont aujourd'hui ces entreprises de taille moyenne qui – dans un souci d'accélérer leur transformation numérique – adoptent en premier les nouvelles technologies. Elles s'équipent donc plus rapidement que les grands groupes – qui ont un process plus lourd et laisse moins de place à la flexibilité. En adoptant, par exemple, l'IoT et les technologies de l'industrie 4.0, ces sociétés "mid market" sont en train de devenir la cible privilégiée des hackers.

Type d'attaque : Des ransomwares liés à l'IoT

Après des années d'observation, on assiste enfin au déploiement à grande échelle de l'IoT. Chambres froides, kiosques, usines, voitures, et même machines de nettoyage industriel, tout cela sera bientôt connecté dans un souci de performance et de monitoring. Espérons qu'ils soient également sécurisés.

Le déploiement de ces dispositifs connectés n'est pas sans risque : leur intégrité peut être compromise si la sécurité n'est pas pensée d'une nouvelle manière. Certaines rumeurs prétendent même que des hackers se sont déjà servis de l'IoT pour attaquer une entreprise et lui demander une rançon. Nous risquons donc de voir une augmentation de ce type d'attaques dans un avenir proche. Par conséquent, l'année 2017 sera certainement la première où une entreprise admettra de façon publique qu'elle a été confrontée à ces cyber-attaques par rançon….[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 : 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

Original de l’article mis en page : Cybersécurité : quels changements pour 2017 ?

Rakos, un nouveau botnet qui vise aussi les Objets connectés

Rakos, un nouveau botnet qui vise aussi les Objets connectés

Après Mirai, voici venir Rakos, un malware infectant des serveurs et des réseaux d'objets connectés, tournant sous Linux, afin de créer des botnets. ET, demain, lancer des attaques DDoS.

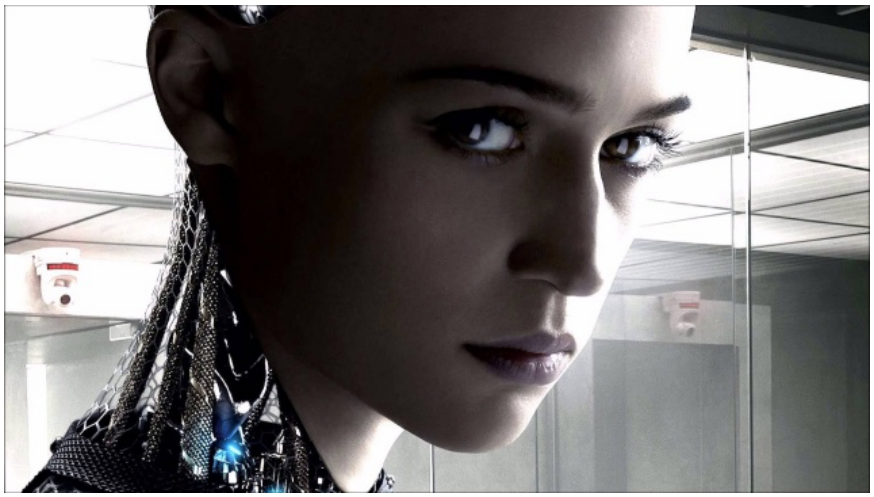
Comme le tristement célèbre malware Mirai, Rakos prend pour cible l'Internet des objets (IoT). Ces deux logiciels malveillants compromettent en effet des serveurs sous Linux et des réseaux d'appareils connectés. La capacité de nuisance de ces botnets contrôlés à distance est bien réelle. Si Mirai se propage essentiellement via les ports logiciels Telnet, Rakos vise lui les ports SSH. Les périphériques embarqués et les serveurs ayant un port SSH ouvert ou un mot de passe très faible sont les plus exposés. Rakos a été découvert cet été par les chercheurs de ESET.

À ce jour, Rakos est utilisé pour mener des attaques par force brute, indique l'entreprise dans un billet de blog. Et ce, afin d'ajouter d'autres appareils compromis à son réseau de machines zombies. Mais le programme pourrait également servir à mener des campagnes de spam ou des attaques par déni de service distribué (DDoS) d'ampleur, comme l'a fait Mirai…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Rakos, un nouveau botnet IoT en constitution

L’Intelligence Artificielle a t-elle le droit de tuer ?



L’Intelligence Artificielle a t-elle le droit de tuer ?

Depuis les prémices de l'Intelligence Artificielle, nous savions qu'un jour ou l'autre que celle-ci devrait prendre des décisions concernant l'intégrité physique d'un être humain. Nous savions et repoussions ce moment où il faudrait fournir une réponse à l'Intelligence Artificielle.
Avant d' aborder le sujet principal, je pense qu' il est nécessaire de rappeler qu'une Intelligence Artificielle prend des décisions en analysant soit des probabilités, soit une base de faits qui lui ont été soumis par l'être humain. C'est une vision réduite et simplifiée. Certes, celle-ci apprend de ses erreurs, mais quand cela concerne l'intégrité humaine, l'erreur peut être fatale.
Nous avons longtemps repoussé ce moment, le voici enfin arrivé avec l'ère des voitures « Autonomes, Connectées, Intelligentes ». Quoi de plus sensible, de plus vital que le droit de tuer. Un « *dominica postestas* » autrefois octroyé aux puissants ou aux maîtres sur leurs esclaves, un droit mettant fin à la vie d'êtres humains. Mais les temps changent, la civilisation évolue, les technologies apparaissent et posent alors de nouveaux dilemmes, celui de tuer va être l'un des plus importants de notre époque. Qui peut se targuer d'un tel droit alors que nous ne faisons pas confiance aux médecins pour accompagner la fin de vie.

Les voitures vont poser le problème suivant : **Qui tuer lors de la confrontation de celles-ci en face à face où aucune échappatoire est possible ?**
Que ce soit voiture contre piéton où l'on a le choix entre :
• Faire sortir la voiture de la route (donc **tuer** ses occupants) et **sauver** le piéton.
• **Percuter** le piéton et **sauver** les personnes à l'intérieur du véhicule.
Ou bien, voiture contre voiture, où là encore deux choix s'opposent :
• les occupants de la voiture A et laisser **saufs** ceux du véhicule B
• les occupants de la voiture B et laisser **saufs** ceux du véhicule A

Je vous propose d' analyser cette situation à travers plusieurs cas :
Cas 1
Confrontation entre une voiture conduite par un homme âgé de 70 ans et une voiture où sont présents une mère et ses deux enfants. Qui tuer ?
Un cas de conscience se pose. Vais-je choisir de tuer l'homme sous prétexte qu'il est âgé et qu' en face, il 'a deux enfants. Inévitablement, la majorité des personnes va alors choisir de tuer l'homme âgé, car les enfants sont sacralisés par l'insouciance, la jeunesse et l'innocence.
Cas 2
Confrontation entre une voiture conduite par une jeune femme et un homme traversant la route sur le passage piéton et donc ayant la priorité. Qui tuer ?
Là, on met en opposition la jeunesse et le bon droit. Doit-on faire primer la jeunesse ou le bon droit ? Doit-on tuer la conductrice ou doit-on tuer l'homme qui traverse de manière anodine le passage piéton ? La tendance va être à tuer la conductrice, car elle ne respecte pas le code de la route.
Cas 3
Confrontation entre deux voitures, une conduite par un homme et une autre par un individu. Qui tuer ?
Là, le mot individu perturbe, qui se cache derrière ? Qui est dans cette voiture ? Quand il' a une inconnue, que faire ? Quelle décision prendre ? Qui tuer ?
Car là est un autre problème, les voitures nouvelle génération, vont mettre du temps à devenir la norme, systèmes interconnectés, oui ! Mais par pour tous, du moins pas dans l'immédiat. Et même s 'ils deviennent omniprésents, qui peut assurer aujourd'hui que nous n'aurons pas de hack ou détournements de ces systèmes.
Étudions un quatrième cas :
Cas 4
Confrontation entre une voiture remplie d 'hommes et une qui annonce un père et ses enfants. Qui tuer ?
On revient sur le fait de la jeunesse, l'innocence, en apparence. Je vous ai volontairement dissimulé une donnée. Il n''y avait qu'**un homme dans la voiture** au père et enfants. Si vous vous êtes dit que vous tuiez inévitablement les occupants de la voiture où se trouvaient les hommes, vous avez agi comme le ferait la majorité. Une intelligence artificielle recevant ces données erronées tuera sûrement les mêmes passagers. **Sauf qu'en face, il y a une personne qui vient de survivre, car elle a trompé le système, car elle a estimé que sa vie valait plus que celle des autres**. Et c' est là qu'on arrive sur **une question de sécurité informatique, celle de l'intégrité de ces systèmes.**

Car quiconque peut modifier ceux-ci peut se donner un probable droit de tuer ! Ceci n'est heureusement que de la fiction à cet instant, mais le détournement de ces systèmes a déjà été prouvé lors de conférences en sécurité informatique. Ces systèmes sont donc des points vitaux de l'Internet des Objets, il doit devenir obligatoire d'assurer une intégrité sans faille sur ceux-ci !…[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 : 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

Original de l'article mis en page : L'Intelligence Artificielle a le droit de tuer… — Hackademics : Forum de hacking — hackers white hat — cours de securite informatique

Utilisez cette carte pour savoir où utiliser votre drone de loisir

	Utilisez cette carte pour savoir où utiliser votre drone de loisir

Cette carte signale toutes les zones de restrictions et dinterdictions…
Le secrétaire d'Etat aux Transports, Alain Vidalies, a annoncé mardi la mise en ligne d'une carte de France interactive représentant les zones interdites ou restreintes pour l'usage de drones de loisir.
La carte est accessible à l'adresse http://www.geoportail.gouv.fr/donnees/restrictions-pour-drones-de-loisir

Outre-mer dans les prochains mois
« A la veille des fêtes de fin d'année, la mise en ligne de cette carte interactive offre une information accessible aux télépilotes pour faire voler leur drone en toute sécurité sur tout le territoire métropolitain », a déclaré Alain Vidalies dans un communiqué.

Cette carte, élaborée par la Direction générale de l'aviation civile (DGAC) avec l'Institut national de l'information géographique et forestière (IGN), définit les zones de restrictions et d'interdictions permanentes en France métropolitaine.
L'outil sera complété, dans les prochains mois, par des cartes des Outre-mer, tandis que l'intégration des zones de restrictions temporaires est à l'étude.

Réagissez à cet article

Original de l'article mis en page : Drones de loisir: Une carte interactive de France pour savoir où les utiliser

En 2017, les pirates informatiques vont mettre les bouchées doubles

En 2017, les pirates informatiques vont mettre les bouchées doubles

Les hackers vont notamment chercher à ébranler la confiance que l'on porte aux données, annonce un rapport de CyberArkBy SHOSHANNA SOLOMON

Les cyber-criminels du monde entier devraient intensifier leur activité l'année prochaine en utilisant l'intelligence artificielle et la manipulation des sources d'information pour créer des attaques plus fortes et plus dévastatrices, mettent en garde les experts de CyberArk.
En infiltrant et en manipulant les sources d'information, les pirates s'efforceront de saper la confiance des gens dans l'intégrité des données qu'ils reçoivent, utiliseront l'intelligence artificielle pour mener des cyber-attaques plus sophistiquées et augmenteront la collaboration entre eux pour déclencher un plus grand désordre, selon les prévisions cybersécuritaires pour 2017.
« L'intégrité de l'information sera l'un des plus grands défis auxquels les consommateurs, les entreprises et les gouvernements du monde devront faire face en 2017, où les informations venant de sources vénérées ne seront plus dignes de confiance », ont déclaré les experts.
« Les cyber-attaques ne se concentreront pas seulement sur une entreprise spécifique, il y aura des attaques contre la société visant à éliminer la confiance elle-même ».
Les attaquants ne se contentent pas d'accéder à l'information : ils « contrôlent les moyens de changer l'information là où elle réside et la manipulent pour les aider à atteindre leurs objectifs », affirment les auteurs.
Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)
Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)
Manipuler l'information – dans une campagne électorale par exemple – peut être un outil puissant. L'altération de contenus inédits, comme les fichiers audio, pourrait conduire à une augmentation des tentatives d'extorsion, en utilisant des informations qui peuvent ne pas être réelles ou prises hors de leur contexte.
« Il sera plus facile que jamais de rassembler des informations réelles volées dans une brèche avec des informations fabriquées, pour créer un déséquilibre ce qui rendra plus difficile pour les gens de déterminer ce qui est réel et ce qui ne l'est pas ».
L'augmentation de l'utilisation mobile, du web et des médias sociaux sont parmi les facteurs clés contribuant à l'augmentation explosive des cyber-menaces, a déclaré MarketsandMarkets, une firme de recherche basée au Texas, dans un rapport. La semaine dernière, Yahoo a subi le plus grand piratage au monde connu à ce jour, dans lequel la société a découvert une violation de sécurité vielle de 3 ans qui a permis à un pirate de compromettre plus d'un milliard de comptes d'utilisateurs.
Le marché mondial de la cyber-sécurité atteindra plus de 170 milliards de dollars d'ici 2020, selon une estimation de MarketsandMarkets, avec des entreprises qui se concentrent globalement sur les solutions de sécurité mais aussi sur les services…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Les pirates informatiques vont mettre les bouchées doubles en 2017 | The Times of Israël