Sécurité des vote électronique en France, comme aux USA ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Sécurité des vote électronique en France, comme aux USA ?				

L'année 2017 sera une grosse année de scrutins, avec l'élection présidentielle en avril-mai et les législatives en juin. Et comme depuis une dizaine d'années qu'un ministre de l'Intérieur, Nicolas Sarkozy, a poussé l'introduction d'ordinateurs de vote en France, des communes vont encore obliger leurs électeurs à voter sur ces machines dont ils ne peuvent contrôler eux-mêmes l'intégrité (en 2012, une soixantaine de communes pour 1,5 million d'électeurs).

Photo: machine à voter utilisée à Stains (Seine-Saint-Denis) aux élections départementales le 22 mars 2015. Chris93/Wikimedia Commons/CC by-sa

Un député socialiste, Sébastien Pietrasanta, vient à cette occasion de poser au gouvernement une question écrite sur « la sécurisation du vote électronique ». Il demande notamment:

« Au-delà d'un risque connu sur la fiabilité des machines et sur la difficulté de recompter les voix, la menace de piratage informatique par des puissances étrangères est hélas d'actualité. Si la menace concerne principalement les partis politiques, à l'instar du piratage des ordinateurs du Parti démocrate aux États-Unis, la possibilité d'une attaque des machines à voter n'est plus à exclure. Aussi, il souhaiterait savoir ce que le ministère de l'intérieur, en charge des élections, compte mettre en place pour assurer la sécurisation du vote lors des élections présidentielle et législatives 2017 et s'il envisage de recourir à un moratoire sur l'utilisation de ces machines électroniques au nom d'un principe de précaution. »

Une position oubliée du PS en 2007

Cette question a été repérée par Nextinpact – qui ironise sur le moratoire « pourtant en vigueur depuis quasiment dix ans », mais il ne s'agit que d'un moratoire sur l'installation du vote électronique dans de nouvelles communes, pas sur son usage dans les villes où il est déjà en place, si c'est dans ce sens que l'entend le député.

Le Parti socialiste, qui en 2007 (quand François Hollande en était premier secrétaire) demandait la suspension du vote électronique, l'a maintenu contre vents et marées depuis son retour au pouvoir en 2012, et indiqué en 2014 encore sa position: ni extension ni abandon (une commune peut choisir de revenir au vote papier, mais au niveau national rien n'est imposé). Donc en 2017, ce sera, encore, circulez il n'y a rien à voir.

La question du député (publiée le 27 décembre) fait référence au piratage du parti démocrate aux Etats-Unis, en pleine actualité puisque c'est une des raisons de l'expulsion de 35 diplomates russes que vient de décider Barack Obama.

L'opacité du vote électronique en soi est aussi un problème crucial: avant l'élection de novembre aux Etats-Unis, un informaticien spécialiste de la sécurité, Bruce Schneier, mettait en garde contre les risques de piratage des machines de vote électronique.

USA: toutes les machines peuvent être piratées

Un reportage de Pixels/Le Monde, depuis le Chaos Computer Congress cite deux chercheurs de l'université du Michigan, Alex Halderman et Matt Bernhard, qui ont participé aux recomptages de certains Etats après le scrutin. S'ils pensent, sans en être certains, que le vote de novembre n'a pas été piraté, ils pointent les nombreuses vulnérabilités du système de vote américain:

« Première faiblesse : les machines à voter. Plus de 50 modèles différents existent et, selon les chercheurs, toutes peuvent être piratées. 'De nombreuses machines à voter ont été étudiées, par des chercheurs indépendants, et dans tous les cas, il a été prouvé que la machine était vulnérable à l'injection de programmes informatiques malveillants faussant les résultats', explique M. Halderman.

Les responsables des élections objectent que ces machines ne sont pas connectées à Internet et sont donc protégées. Cela ne fait aucune différence, explique M. Bernhard, puisque est insérée dans chaque machine, et avant chaque scrutin, une carte mémoire contenant les paramètres du vote. C'est aussi dans cette carte que sont stockés les résultats. Or, les ordinateurs qui paramètrent ces cartes sont fréquemment connectés à Internet. »

Autre faiblesse, l'absence de contrôle a posteriori: plus de 70% des votes aux Etats-Unis ont une trace en papier. « Il faudrait comparer les votes contenus dans les cartes mémoires et la trace en papier, mais malheureusement la plupart des Etats ne le font pas. » Un peu comme en France: le meilleur moyen de prétendre que le vote électronique a bien marché, c'est de ne surtout pas vérifier après coup…[lire la suite]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

Vous avez un doute sur la sécurité de vos machines à voter ?
Vous souhaitez un expert indépendant spécialisé en votes électroniques pour expertiser le système de vote électronique que vous avez choisi ?
Nous pouvons expertiser leur sécurité en rapport avec la délibération de la CNIL n° 2010-371 du 21 octobre 2010.
Contactez-nous

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l’article mis en page : Vote électronique: en France, aux USA, tout baigne? Hum… – ZDNet

---

Le réseau électrique américain pénétré par des pirates Russes

Washington – Des pirates informatiques russes sont parvenus à pénétrer le réseau électrique américain via un fournisseur du Vermont, une cyberattaque sans conséquence sur les opérations de cette entreprise mais qui a pu révéler une « vulnérabilité », rapporte vendredi le Washington Post.

« Un code associé à l'opération de piratage informatique baptisée Grizzly Steppe par l'administration Obama a été détecté à l'intérieur du système d'un fournisseur d'électricité du Vermont », écrit le quotidien sur son site Internet, sans indiquer de date.
Se référant à des responsables américains non identifiés, il souligne que ce si code *« n'a pas été activement utilisé pour perturber les opérations du fournisseur* […] *la pénétration du réseau électrique national est importante parce qu'elle représente une vulnérabilité potentiellement grave ».*
Les autorités américaines ignorent à ce stade quelles étaient les intentions des Russes, poursuit le *Washington Post*, supputant qu'ils pourraient avoir tenté de porter atteinte aux activités du fournisseur –non identifié par les sources du journal– ou qu'il pourrait simplement s'agir d'un test de faisabilité.
Selon le journal, le Vermont compte deux importants fournisseurs d'électricité : Green Mountain Power et Burlington Electric.
Les pirates russes auraient envoyé des emails pour piéger les destinataires, leur faisant révéler leurs mots de passe.
En décembre 2015, 80 000 habitants de l'ouest de l'Ukraine avaient été plongés plusieurs heures dans le noir à la suite d'une cyberattaque d'une ampleur inédite. Les Russes avaient été désignés comme en étant les auteurs, ce qu'ils avaient nié…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Des pirates russes ont pénétré le réseau électrique américain | Le Devoir

Alerte : Un hack par MMS bloque l’application Messages de votre iPhone

	Alerte : Un hack par MMS bloque l’application Messages de votre iPhone

Un nouveau hack iPhone permet de bousiller à distance l'application Messages, qui permet d'envoyer et de recevoir les textos et MMS. Il s'agit d'un fichier .vcf (une fiche contact) corrompue, qui semble complètement faire flipper votre application Message, qui freeze, avant devenir complètement inutilisable. Même un redémarrage de l'iPhone ne vient pas à bout du problème qui touche tous les iPhone sous toutes les versions d'iOS 9 et d'iOS 10, y compris les versions bêta.

Dans la vidéo Youtube que vous pouvez voir en fin d'article, @Vicedes3 montre un nouveau hack à distance des iPhone assez embarrassant. En fait, l'ouverture d'une fiche contact viciée envoyée par MMS suffit à rendre l'application Messages, vitale pour envoyer et recevoir des messages, complètement inutilisable. Le redémarrage du terminal, voire même un hard reset n'y feront rien.
Nous vous recommandons donc de ne pas vous amuser à l'essayer sur votre iDevice. Pour que vous compreniez ce qui se passe, ce fichier .vcf est en fait extrêmement lourd, et excède des limites de taille qu'Apple a tout simplement omis de définir. Du coup, ce fail devrait être relativement simple à corriger. Apparemment, toutes les versions d'iOS 9 et 10, même les bêtas les plus récentes sont concernées par ce problème.
Personne n'ayant eu auparavant l'idée d'exploiter la taille des fiches contact, la faille serait ainsi tout simplement passée inaperçue pendant tout ce temps. La seule manière de réellement se protéger, c'est de ne surtout pas ouvrir les fiches contact reçues depuis des sources autres que vos contacts de confiance. Ce n'est pas en soit un virus, donc si vous le recevez, c'est que quelqu'un vous fait une mauvaise blague…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : iPhone : ce nouveau hack par MMS bousille votre application Messages

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 entrainant 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]

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

---

A 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 la 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 28% 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

---

Réagissez à cet article

Tendances actuelles et émergentes pour la cybersécurité en 2017

Tendances actuelles et émergentes pour la cybersécurité en 2017

L'année 2016 a été marquée par un grand nombre de cyberattaques très diverses, allant d'attaques de type DDoS par le bais de caméra de sécurité connectées, jusqu'au supposé piratage de partis politiques durant les élections américaines. Nous avons aussi constaté une forte augmentation des fuites de données, aussi bien au niveau des petites que des grandes organisations, avec des pertes significatives de données personnelles des utilisateurs. En cette fin d'année, nous réfléchissons donc aux directions que vont prendre ces tendances en 2017.

Les tendances actuelles et émergentes :

Les attaques destructives de type DDoS utilisant les objets connectés vont augmenter.

En 2016, Mirai a montré le potentiel destructeur important que pouvaient avoir les attaques DDoS, du fait notamment du manque de sécurité des objets connectés. Les attaques de Mirai exploitaient seulement un faible nombre d'équipements et de vulnérabilités, en utilisant des techniques simples pour deviner les mots de passe. Cependant, d'autres cybercriminels n'auront aucun mal à étendre la portée de ce type d'attaque, du fait du nombre considérable d'objets connectés contenant des codes obsolètes, ainsi que des applications et systèmes d'exploitation non mis à jour contenant souvent des vulnérabilités bien connues. Il faut s'attendre à une utilisation plus systématique des exploits présents au sein des objets connectés et de techniques avancées permettant de deviner les mots de passe, pour compromettre une plus grande variété d'objets connectés, afin de mener des attaques de type DDoS ciblant d'autres équipements connectés à votre réseau.

Les attaques ciblées d'ingénierie sociale seront plus sophistiquées.

Les cybercriminels sont de plus en plus expérimentés pour exploiter la première des vulnérabilités : l'être humain. Des attaques ciblées de plus en plus sophistiquées et convaincantes cherchent à duper et à amadouer les utilisateurs, afin de les pousser à se mettre en danger eux-mêmes. Par exemple, il est courant de voir des emails s'adressant à leurs destinataires par leurs noms et qui prétendent que ces derniers ont une dette impayée, que l'expéditeur en question serait autorisé à collecter. La peur, l'intimidation et les menaces de recouvrement au nom de la loi, sont des tactiques très utilisées et assez classiques. L'email en question vous redirige alors vers un lien malveillant, sur lequel les utilisateurs cliquent dans la panique, amorçant alors l'attaque. De telles attaques par hameçonnage (phishing), ne peuvent plus être détectées à la lecture par de simples erreurs grossières commises par les cybercriminels.

Les infrastructures financières deviendront des cibles privilégiées.

Les attaques ciblées de phishing, et particulièrement celles ciblant les dirigeants (whaling), vont continuer de croitre. Ces attaques utilisent des informations détaillées concernant les dirigeants d'entreprises, afin de duper les employés et les inciter à envoyer de l'argent à des cybercriminels, ou à compromettre certains comptes bancaires. Nous nous attendons aussi à voir davantage d'attaques ciblant des infrastructures financière sensibles, telles que l'attaque ayant pris pour cible les institutions connectées au système SWIFT, qui a coûté à la banque centrale du Bangladesh 81 millions $, en février dernier. SWIFT a récemment admis que d'autres attaques de ce type avaient eu lieu, et qu'il s'attendait à en voir davantage en déclarant, dans une lettre adressée aux clients de la banque : « La menace est très persistante, adaptative et sophistiquée. Il faut s'attendre à ce qu'elle continue de sévir. ».

L'exploitation de l'infrastructure intrinsèquement non sécurisée d'Internet va se poursuivre.

Tous les internautes font encore confiance à de vieux protocoles fondateurs, que leur omniprésence empêche de réorganiser ou de remplacer. Ces protocoles archaïques qui ont pendant longtemps été les piliers de l'Internet et des réseaux professionnels sont aujourd'hui fragilisés, parfois d'une manière surprenante. Par exemple, les attaques contre BGP (Border Gateway Protocol) auraient pu, en théorie, perturber ou même mettre hors service une bonne partie du Web. Les attaques DDoS visant Dyn en octobre dernier (lancées depuis une multitude d'objets connectés) ont mis hors service un fournisseur majeur de services DNS, et ont de ce fait rendu inaccessible une partie de l'Internet. Il s'agissait de l'un des plus importants assauts jamais observés, et ceux à l'origine de ces attaques ont déclaré qu'il s'agissait seulement d'un coup d'essai. Les fournisseurs d'accès Internet et les entreprises peuvent bien évidemment prendre des mesures pour se protéger, mais pourraient trouver difficile d'éviter tous les dégâts importants potentiellement causés par des individus ou des états qui auront choisi d'exploiter les failles de sécurité les plus profondes du Web.

La sophistication des attaques va augmenter.

Le nombre d'attaques continue à augmenter, avec une sophistication croissante des techniques et de l'ingénierie sociale, qui reflète une analyse minutieuse et répétée des organisations et des réseaux de leurs victimes. Les cybercriminels peuvent compromettre de nombreux serveurs et stations de travail bien avant de commencer à voler des données ou agir de façon plus agressive. Ces attaques, en général pilotées par des experts, sont plus stratégiques que tactiques, et peuvent au final causer des dommages considérables. Il s'agit ici d'un monde très différent des attaques par malwares programmés et automatisés dont nous avons l'habitude. C'est un monde où la stratégie et la patience jouent un rôle beaucoup plus important pour échapper aux détections.

De plus nombreuses attaques utiliseront des outils d'administration intégrés.

Nous voyons davantage d'exploits basés sur PowerShell, le langage et kit de développement de Microsoft pour l'automatisation des tâches administratives. En tant que langage de script, PowerShell contourne les détections visant les exécutables. Nous voyons également plus d'attaques utilisant des tests de pénétration et d'autres outils d'administration existants, sans qu'ils soient à priori infiltrés et en général suspectés. Ces outils puissants demandent une vigilance toute particulière et des contrôle plus robustes.

Les ransomwares vont continuer à progresser.

Comme de plus en plus d'utilisateurs sont conscients de l'existence du risque d'attaques par ransomware via les emails, les cybercriminels exploitent d'autres vecteurs. Certains expérimentent des malwares qui infectent à nouveau le système ultérieurement, longtemps après que la rançon ait été payée. D'autres commencent à utiliser des outils intégrés, à la place de malwares exécutables, afin d'éviter d'être détectés par les solutions de protection Endpoint qui se focalisent sur des fichiers exécutables. De récents exemples ont proposé de déchiffrer les fichiers de leurs victimes si elles acceptaient de diffuser le ransomware vers deux autre contacts, et que ces personnes acceptent de payer. Les ransomwares commencent également à utiliser des techniques autres que le chiffrement, par exemple en détruisant ou corrompant les en-têtes de fichiers. Qui plus est, avec le grand nombre de ransomwares qui persistent sur le Web, les utilisateurs peuvent se retrouver victimes d'attaques sans espoir de pouvoir payer en dernier recours, car le système de paiement ne fonctionne plus.

Des attaques visant des objets personnels connectés vont émerger.

Les utilisateurs d'objets connectés domestiques s'imaginent rarement que leur veilleuse écoute-bébé puisse être piratée pour attaquer des sites internet. Cependant, dès qu'un pirate contrôle un équipement connecté à un réseau domestique, il peut plus facilement pirater d'autres équipements de ce réseau, tels que des ordinateurs portables contenant des données personnelles sensibles. Nous nous attendons à voir plus d'attaques de ce genre, ainsi que des attaques impliquant des caméras vidéo ou des microphones afin d'espionner les foyers. Les cybercriminels trouvent toujours un moyen de tirer profit de leurs attaques.

Le malvertising et la corruption des écosystèmes de publicités en ligne vont s'étendre.

Le malvertising, qui fonctionne en répandant des malwares sur les réseaux publicitaires et les pages web, existe déjà depuis plusieurs années. Cependant, nous avons pu observer en 2016 une recrudescence de ce phénomène. Ces attaques mettent en évidence des problèmes plus importants au sein de l'écosystème des publicités en ligne, telle que la fraude au clic, qui génère des clics payants et ne correspondent pas en réalité aux véritables centres d'intérêts de l'internaute. Le malvertising a engendré la fraude au clic, mettant les utilisateurs en danger et abusant les annonceurs par la même occasion.

La diffusion du chiffrement entrainera des problèmes collatéraux.

Le chiffrement se diffuse très largement et il est devenu plus difficile pour les solutions de sécurité d'inspecter le trafic, facilitant ainsi la vie des cybercriminels qui cherchent à s'infiltrer sans être repérés. Sans surprise, les cybercriminels utilisent le chiffrement de manière créative. Les produits de sécurité vont devoir rapidement intégrer les protections réseaux et client afin de pouvoir détecter des évènements pouvant affecter la sécurité après que le code ait été déchiffré au niveau des systèmes Endpoint.

Les cybercriminels s'intéresseront aux exploits des systèmes virtualisés dans le Cloud.

Les attaques contre des composants physiques (exemple de Rowhammer) ouvrent la voie à de nouveaux exploits potentiellement dangereux contre des systèmes cloud virtualisés. Les cybercriminels peuvent abuser d'un hôte ou bien d'un invité sur un système hôte partagé, attaquer la gestion des privilèges et potentiellement accéder aux données de tiers. De plus, comme Docker et les écosystèmes de conteneurs logiciels (« serverless ») deviennent de plus en plus populaires, les cybercriminels vont certainement se mettre à chercher des failles à exploiter dans le cadre de cette nouvelle tendance des systèmes d'information. Nous nous attendons donc à voir des tentatives actives pour rendre de telles attaques opérationnelles.

Des attaques techniques visant les Etats et les populations apparaîtront. Les attaques technologiques sont devenues hautement politiques. Les populations doivent faire face à des risques grandissants en matière de désinformation (« les fausses nouvelles ») et concernant les systèmes de vote. Par exemple, les experts ont démontré l'existence d'attaques permettant à un électeur, au niveau local, de voter de manière répétitive sans aucune détection. Même si les Etats n'organisent jamais d'attaques contre leurs adversaires aux élections, le sentiment que ce type d'attaques puisse exister est en soi une arme puissante…[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

---

Réagissez à cet article

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

---

Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

La dernière étude dIFS sur les défis auxquels les DSI sont confrontés durant la période des fêtes de fin d'années révèle que 76% des sondés se sentent davantage préoccupés à l'approche de cette période et ce, pour plusieurs raisons : la disponibilité du personnel (41% des répondants), les risques de piratage liés à la sécurité IT (31%) ainsi que les besoins IT des collaborateurs travaillant à distance (31% également). Tout cela a un impact certain sur les processus et activités métier.

De tous, les plus inquiets quant à la disponibilité du personnel à la période des fêtes de fin d'année sont les français. 62% d'entre eux déclarent qu'il s'agit de l'une de leurs plus grandes préoccupations au cours de la saison des fêtes de fin d'année. Á l'opposé, près de la moitié des répondants américains (48%) citent le piratage informatique.

Du côté des « besoins », 42% des décideurs IT sont en demande d'un budget plus important. La migration vers le Cloud (18%) et le recrutement de personnel IT (16%) sont également cités dans le top 3 de leurs besoins. Par ailleurs, un quart des répondants américains et suédois (respectivement 26% et 25%) souhaitent, à court terme, une accélération de la migration vers le Cloud, alors qu'ils ne sont que 11% et 14% en Australie et Allemagne à privilégier cet enjeu.

« Ce qui ressort clairement de notre étude est que de nombreux décideurs IT ont des craintes légitimes pour la période des fêtes de fin d'année : disponibilité du personnel, risque de piratage informatique, commente Mark Boulton, CMO d'IFS. Il est essentiel que toutes les entreprises, quelle que soit leur taille, se préparent à affronter les problèmes qui pourraient survenir et soient en mesure d'accompagner, à distance, leurs collaborateurs ». L'IoT et la migration vers le Cloud faisant partie des solutions possibles.

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

---

Réagissez à cet article

Original de l'article mis en page : Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

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

Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?

	Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?

Suite à une nouvelle panne de courant, la compagnie nationale d'électricité de l'Ukraine enquête pour savoir si une attaque de cyberpirates est à l'origine du problème.
Des experts en sécurité cherchent à savoir si la panne de courant qui a affecté ce week-end certains quartiers de la capitale ukrainienne, Kiev, et la région environnante provient d'une cyberattaque. Si ce dernier point venait à être confirmé, il s'agirait du deuxième black-out causé par des pirates informatiques en Ukraine, après celle qui s'est produite en décembre 2015.

L'incident a affecté les systèmes de commande d'automatisation d'un relais de puissance près de Novi Petrivtsi, un village situé au nord de Kiev, entre samedi minuit et dimanche. Cela a entraîné une perte de puissance complète pour la partie nord de Kiev sur la rive droite du Dniepr et la région environnante…

75 minutes pour rétablir le courant

Les ingénieurs d'Ukrenergo, la compagnie d'électricité ukrainienne, ont commuté l'équipement de commande en mode manuel et commencé à rétablir la puissance par palier de 30 minutes, a dit Vsevolod Kovalchuk, directeur d'Ukrenergo, dans un billet posté sur Facebook. Il a fallu 75 minutes pour restaurer toute la puissance électrique dans les zones touchées de la région, où les températures descendent jusqu'à -9 en ce moment. Une des causes suspectées est « une interférence externe à travers le réseau de données » a déclaré sans plus de précision Vsevolod Kovalchuk. Les experts en cybersécurité de la société étudient la question et publieront très bientôt un rapport.
Parmi les causes possibles de l'accident figurent le piratage et un équipement défectueux, a déclaré Ukrenergo dans un communiqué. Les autorités ukrainiennes ont été alertées et mènent une enquête approfondie. En attendant, les premières conclusions, tous les systèmes de commande ont été basculés du mode automatique au manuel, a indiqué la compagnie.

Un Etat derrière les attaques sophistiquées

Si un piratage venait à être confirmé, ce serait la seconde cyberattaque en un an contre le réseau électrique ukrainien. En décembre dernier, juste avant Noël, des pirates informatiques avaient lancé une attaque coordonnée contre trois compagnies d'électricité régionales ukrainiennes. Ils avaient réussi à couper l'alimentation de plusieurs sous-stations, provoquant des pannes d'électricité qui ont duré entre trois et six heures et touché les résidents de plusieurs régions.
A l'époque, les services de sécurité ukrainiens, le SBU, avaient attribué l'attaque à la Russie. Bien qu'il n'y ait aucune preuve définitive liant ces attaques au gouvernement russe, les cyberattaquants avaient utilisé un morceau de malware d'origine russe appelé BlackEnergy, et la complexité de l'attaque suggère l'implication d'un État. La semaine dernière, des chercheurs du fournisseur de sécurité ESET ont alerté la communauté au sujet d'attaques récentes contre le secteur financier ukrainien menées par un groupe qui partage de nombreuses similitudes avec le groupe BlackEnergy…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une cyberattaque suspectée de causer un black-out en Ukraine – Le Monde Informatique

---

Que nous réserve la CyberSécurité en 2017 ?

Que nous réserve la CyberSécurité en 2017 ?

La fin de l'année c'est aussi et surtout la période des bilans. Dans cet article, nous mettrons en évidence les cinq tendances les plus importantes tendances à venir. Qu'elles se maintiennent ou évoluent durant l'année 2017, une chose est sûre, elles risquent de donner du fil à retordre aux professionnels de la cybersécurité.

1 : intensification de la guerre de l'information
S'il y a bien une chose que la cybersécurité nous a apprise en 2016, c'est que désormais, les fuites de données peuvent être motivées aussi bien par la recherche d'un gain financier ou l'obtention d'un avantage concurrentiel que pour simplement causer des dommages dus à la divulgation d'informations privées. À titre d'exemples, le piratage du système de messagerie électronique du Comité National Démocrate (DNC) américain qui a conduit à la démission de Debbie Wassermann Schultz de son poste de présidente ; ou encore, la sécurité des serveurs de messagerie qui a miné la campagne présidentielle américaine de la candidate Hillary Clinton dans sa dernière ligne droite. Il est également inexcusable d'oublier que Sigmundur Davíð Gunnlaugsson, le Premier ministre islandais, a été contraint de démissionner en raison du scandale des Panama Papers.
Les évènements de ce type, qui rendent publiques de grandes quantités de données dans le cadre d'une campagne de dénonciation ou pour porter publiquement atteinte à un opposant quelconque d'un gouvernement ou d'une entreprise, seront de plus en plus fréquents. Ils continueront de perturber grandement le fonctionnement de nos institutions et ceux qui détiennent actuellement le pouvoir.

2 : l'ingérence de l'État-nation
Nous avons assisté cette année à une augmentation des accusations de violations de données orchestrées par des États-nations. À l'été 2015, l'administration Obama a décidé d'user de représailles contre la Chine pour le vol d'informations personnelles relatives à plus de 20 millions d'Américains lors du piratage des bases de données de l'Office of Personnel Management. Cette année, le sénateur américain Marco Rubio (républicain, État de Floride) a mis en garde la Russie contre les conséquences inévitables d'une ingérence de sa part dans les élections présidentielles.
Il s'agit là d'une autre tendance qui se maintiendra.
Les entreprises doivent donc comprendre que si elles exercent ou sont liées de par leur activité à des secteurs dont les infrastructures sont critiques (santé, finance, énergie, industrie, etc.), elles risquent d'être prises dans les tirs croisés de ces conflits.

3 : la fraude est morte, longue vie à la fraude au crédit !
Avec l'adoption des cartes à puces – notamment EMV (Europay Mastercard Visa) – qui a tendance à se généraliser, et les portefeuilles numériques tels que l'Apple Pay ou le Google Wallet qui sont de plus en plus utilisés, les fraudes directes dans les points de vente ont chuté, et cette tendance devrait se poursuivre. En revanche, si la fraude liée à des paiements à distance sans carte ne représentait que de 9 milliards d'euros en 2014, elle devrait dépasser les 18 milliards d'ici 2018.
Selon l'article New Trends in Credit Card Fraud publié en 2015, les usurpateurs d'identité ont délaissé le clonage de fausses cartes de crédit associées à des comptes existants, pour se consacrer à la création de nouveaux comptes frauduleux par l'usurpation d'identité. Cette tendance devrait se poursuivre, et la fraude en ligne augmenter.
Le cybercrime ne disparaît jamais, il se déplace simplement vers les voies qui lui opposent le moins de résistance. Cela signifie, et que les fraudeurs s'attaqueront directement aux systèmes de paiement des sites Web.

4 : l'Internet des objets (IdO)
Cela fait maintenant deux ans que les experts prédisent l'émergence d'un ensemble de risques inhérents à l'Internet des objets. Les prédictions sur la cybersécurité de l'IdO ont déjà commencé à se réaliser en 2016. Cela est en grande partie dû à l'adoption massive des appareils connectés d'une part par les consommateurs, mais aussi par les entreprises. En effet, d'après l'enquête internationale portant sur les décideurs et l'IdO conduite par IDC, environ 31 % des entreprises ont lancé une initiative relative à l'IdO, et 43 % d'entre elles prévoient le déploiement d'appareils connectés dans les douze prochains mois. La plupart des entreprises ne considèrent pas ces initiatives comme des essais, mais bien comme faisant partie d'un déploiement stratégique à part entière.
Cette situation va considérablement empirer. L'un des principaux défis de l'IdO n'est pas lié à la sécurisation de ces appareils par les entreprises, mais plutôt au fait que les fabricants livrent des appareils intrinsèquement vulnérables : soit ils sont trop souvent livrés avec des mots de passe par défaut qui n'ont pas besoin d'être modifiés par les utilisateurs, soit la communication avec les appareils ne requiert pas une authentification de niveau suffisant ; ou encore, les mises à jour des firmwares s'exécutent sans vérification adéquate des signatures. Et la liste des défauts de ces appareils n'en finit pas de s'allonger.
Les entreprises continueront d'être touchées par des attaques directement imputables aux vulnérabilités de l'IdO, que ce soit par des attaques par déni de service distribué (attaques DDoS), ou par le biais d'intrusions sur leurs réseaux, rendues possibles par les « faiblesses » inhérentes de l'IdO.

5 : bouleversements de la réglementation…[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

---

Réagissez à cet article

Original de l’article mis en page : Les grandes tendances 2017 de la cybersécurité, Le Cercle