Les pirates ciblent désormais l'Internet of Things | Le Net Expert Informatique

Les pirates ciblent désormais l'Internet of Things

Les assaillants sur internet recourent généralement à des attaques DDos. Mais avec la percée de l'internet des choses (IoT), ils se tournent à présent vers de nouvelles techniques.

DDoS continue de gagner en popularité et évolue aussi. L'année dernière, il s'agissait surtout d'attaques exploitant brièvement une large bande passante. Aujourd'hui, les attaques font moins de 10 Gbps, mais durent plus de 24 heures. Voilà ce qu'affirme Akamai dans son tout dernier rapport State of the Internet.

« Ce type d'attaque de longue durée va souvent de pair avec par exemple des demandes de versement d'une somme d'argent. Car si un site ou un service web est paralysé, le fournisseur perd également de l'argent », déclare Tim Vereecke, senior solutions engineer chez Akamai. L'augmentation des attaques est partiellement due au fait que louer un botnet devient plus abordable pour les criminels. « Le coût initial d'exécution d'une attaque DDoS est à présent inférieur à ce qu'il était avant. Voilà qui explique pourquoi on enregistre aujourd'hui davantage d'attaques de plus longue durée, mais qui sont en moyenne moins puissantes. »

Il n'empêche que les attaques lourdes ne restent pas exceptionnelles. C'est ainsi qu'Akamai a encore enregistré au trimestre dernier huit attaques dépassant les 100 Gbps, dont la plus importante atteignait même 170 Gbps.

Mais les pirates semblent déplacer leur intérêt pour DDos vers SSDP (Simple Service Discovery Platform), un protocole pour l'Internet of Things. Ce protocole s'assure entre autres que votre ordinateur reconnaisse les autres appareils internet dans la maison. « Mais ce protocole est aussi conçu pour recevoir toutes sortes de données, ce qui en fait un candidat idéalement utilisable comme intermédiaire pour une attaque. »

Concrètement, vingt pour cent de l'ensemble des attaques recensées au premier trimestre de cette année ont été lancées via SSDP. Et ce, alors que la technique ne s'était même pas manifestée dans les statistiques jusqu'à la seconde moitié de 2014. La solution pour éviter ces attaques, c'est une bonne sécurisation et configuration des appareils connectés entre eux et à internet.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://datanews.levif.be/ict/actualite/les-pirates-ciblent-l-internet-of-things/article-normal-397387.html

l’Expert Informatique obligatoire pour valider les systèmes de vote électronique | Denis JACOPINI

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d’une recommandation relative à la sécurité des systèmes de vote électronique indique que tout système de vote électronique doit faire l’objet d’une expertise indépendante.

Le 30 juin dernier, nous avons suivi notre nième formation 8 rue Vivienne à Paris, dans les locaux de la CNIL. Cette fois, c’était un atelier vote électronique consistant à nous enseigner les bonnes pratiques à mettre en oeuvre dans l’expertise d’un système de vote électronique.

Expert informatique assermenté, Denis JACOPINI peut vous accompagner dans cette démarche d’expertise de systèmes de votes électroniques.

Cette journée de formation, à destination des Experts Informatiques et Experts Judiciaires en Informatique, portait sur le vote électronique. Vous trouverez ci-dessous un résumé de ce que nous considérons essentiel.

Le vote électronique, souvent via internet, connaît un développement important depuis plusieurs années, notamment pour les élections professionnelles au sein des entreprises.

La mise en place des traitements de données personnelles nécessaires au vote doit veiller à garantir la protection de la vie privée des électeurs, notamment quand il s’agit d’élections syndicales ou politiques.

La CNIL souligne que le recours à de tels systèmes doit s’inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin (sauf pour les scrutins publics), le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l’élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Les mesures de sécurité sont donc essentielles pour un succès des opérations de vote mais mettent en œuvre des mesures

compliquées, comme par exemple l'utilisation de procédés cryptographiques pour le scellement et le chiffrement.

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que **tout système de vote électronique doit faire l'objet d'une expertise indépendante**.

Par ailleurs, l'article R2314-12 du Code du Travail créé par Décret n°2008-244 du 7 mars 2008 – art. (V) fixe très clairement que préalablement à sa mise en place ou à toute modification substantielle de sa conception, **un système de vote électronique est soumis à une expertise indépendante**. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Information complémentaire : Les articles R2314-8 à 21 et R2324-4 à 17 du Code du Travail indiquent de manière lus générale les modalités du vote électronique lors du scrutin électoral de l'élection des délégués du personnel et des délégués du personnel au comité d'entreprise.

Ces dispositions ont été complétées par la délibération 2010-371 de la CNIL du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération et notamment sur :

- le code source du logiciel y compris dans le cas de l'utilisation d'un logiciel libre,
- les mécanismes de scellement utilisés aux différentes

étapes du scrutin (voir ci-après),
- le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
- les échanges réseau,
- les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- Être un informaticien spécialisé dans la sécurité ;
- Ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser la solution de vote ;
- Posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- Avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondants à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de

vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

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

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

Les atteintes aux libertés de la Loi Renseignement | Le Net Expert Informatique

Les atteintes aux libertés de la Loi Renseignement

Hier, le Sénat a commencé l'examen du projet de loi sur le renseignement par l'inévitable discussion générale. Chacun des groupes et sénateurs a pu ainsi donner « sa » religion sur ce texte, contesté par bon nombre d'organisations de la société civile, tout comme la CNIL ou le défenseur des droits. Compte rendu.

D'entrée, Manuel Valls a jugé le texte comme indispensable afin d'apporter la précision et l'encadrement nécessaire aux activités des services du renseignement, dans un contexte d'évolution technologique : « Il faut pouvoir suivre les terroristes sur leurs réseaux, car ils utilisent tous les outils du numérique pour leurs actions de propagande et d'embrigadement, ainsi que pour échanger. C'est pourquoi nous autorisons le recours aux algorithmes : afin de détecter des terroristes jusqu'alors inconnus et des individus connus qui recourent à des techniques de dissimulation. Moins d'un djihadiste sur deux avait été détecté avant son départ en Syrie ; nous devons pouvoir faire mieux. »

Quand Philippe Bas s'attaque aux « inoculations toxiques »

Des propos à comparer à ceux de Philippe Bas (UMP), rapporteur du texte : « **Le texte confronte les intérêts fondamentaux de la Nation et la sauvegarde de la vie humaine aux exigences aussi fortes que sont le respect de la vie privée et la garantie des libertés fondamentales. Il donne un cadre légal aux services de renseignement** » s'est-il félicité, en pleine phase avec le gouvernement. S'en prenant aux détracteurs, il jure cependant que ce projet « ne renforce pas les moyens des services de renseignement, ce n'est pas son objet. Il n'a rien à voir avec la caricature qui en a été faite. Les critiques qui lui sont faites, cependant, sont autant d'anticorps pour que l'État de droit résiste à des inoculations toxiques pour les libertés ».
Une erreur d'analyse patente puisque le projet de loi vise bien à décupler les moyens des services du renseignement, au motif ou prétexte de leur encadrement.

Renseignement, Google, même combat

Yves Detraigne (UDI-UC) s'en est tout autant pris aux opposants à ce texte qui condamnent l'usage des algorithmes, « dont l'utilisation quotidienne, à des fins mercantiles, par les géants du web tels que Google, ne provoque pas les mêmes réactions ». Comme si Google pouvait vous envoyer en prison… Jean-Jacques Hyest (UMP) a pris pour cible la presse et les discours anxiogènes amplifiés lors d'une précédente loi sécuritaire: « On annonçait une catastrophe pour les libertés publiques, c'était « l'horreur » – alors que l'article 13 est plus protecteur des libertés publiques que le droit qui prévalait jusque-là. » Tellement protecteur que cet article (devenu l'article 20), qui autorise l'aspiration de données de connexion par le renseignement, est actuellement en voie de QPC au Conseil d'État. La Quadrature du Net, FDN et FFDN ayant victorieusement fait valoir aux yeux du rapporteur que certains droits et libertés fondamentaux étaient un peu trop menacés par ces mécanismes, qui servent de socles juridiques à la loi Renseignement.

Il y aura des faux positifs et des atteintes aux libertés

Pierre Charon (UMP) admet sans sourciller que des « faux positifs » seront possibles avec les boites noires (algorithme détectant les premières traces de menace terroriste). Mais pas grave : « Cela confirme que nos services ont aussi besoin de moyens humains » et que « les citoyens doivent avoir des voies de recours ». Analyse similaire chez Jean-Pierre Sueur (PS) qui explique que les atteintes aux libertés sont nécessaires : « Vous savez qu'il existe des sites dangereux parce qu'ils encouragent à l'oeuvre de mort. Je crois l'atteinte aux libertés nécessaire pour combattre le terrorisme, pourvu qu'elle soit limitée par le droit ». La question du terrorisme cependant n'est qu'un petit versant de ce texte qui autorise l'espionnage pour d'autres fins, notamment celle de la défense ou la promotion des intérêts français.

Le germe d'une collecte massive débouchant sur une surveillance généralisée

La sénatrice Michelle Demessine (CRC) sera pour sa part plus critique : « ce texte porte en lui le germe d'une collecte massive et indifférenciée de données qui débouche inévitablement sur une surveillance généralisée de la société. ». Claude Malhuret (UMP) embraye, plus réservé encore : « On nous dit que ne seraient concernées que les métadonnées. Cela relève de l'escroquerie intellectuelle. M. X, marié, se connecte tous les quinze jours à un site de rencontres extra-conjugales ; M. Y, dans la même situation, visite toutes les semaines un site de rencontres homosexuelles. Les métadonnées contiennent toute l'information intéressante. Point besoin de connaître aussi le contenu ».

Le sénateur s'est d'ailleurs appuyé sur les (pseudos) reculades aux États-Unis en matière de renseignement pour justement torpiller le pas de danse français. « Nous ne sommes plus loin des horreurs décrites par Orwell après la révélation par Edward Snowden des pratiques de la NSA » ajoute Catherine Morain-Desailly (UDI-UC). « Ce texte est bien un Patriot Act à la française, pris en hâte après les attentats de janvier. Les algorithmes sont source d'erreur, on le sait. Pourquoi les légaliser quand le Congrès américain le refuse désormais ? Supprimons le contrôle par les boites noires qui fragilisent la sécurité des données des entreprises et des institutions à cause des failles que les cybercriminels savent exploiter. Instituons un contrôle de la CNIL, le seul rempart contre l'arbitraire, l'hypersurveillance et l'hypervigilance ».

C'est quoi le programme ?

Les sénateurs débattront véritablement des articles et des amendements à partir de 14 h 30 aujourd'hui jusqu'au 9 juin. Ensuite « leur » texte sera arbitré avec celui des députés en Commission mixte paritaire. Si le gouvernement le souhaite, c'est l'Assemblée nationale qui pourra avoir le dernier mot, du moins si la disharmonie perdure. Après cela, le projet de loi devrait être contrôlé par le Conseil constitutionnel, avant sa publication au Journal officiel. Une promesse de François Hollande, alors que plus de 60 députés se sont déjà réunis pour doubler cette saisine par une action parlementaire en ce sens. Ajoutons que le Conseil constitutionnel pourrait dans le même temps examiner le recours précité, initié par la Quadrature du Net, la FDN et FFDN, si du moins le Conseil d'État suit l'avis du rapporteur général en ce sens (notre compte rendu et l'interview de Me Spinosi)

Source : http://www.nextinpact.com/news/95299-loi-renseignement-faux-positifs-atteintes-aux-libertes-pas-grave.htm
Par Marc Rees

L'analyse comportementale, la nouvelle cyber-arme ? | Le Net Expert Informatique

IdentityGRC 2015 est la dernière offre de détection comportementale de la fraude et de la fuite de données de Brainwave, co-fondée par Sébastien Faivre. (crédit : D.R.)

L’analyse comportementale, la nouvelle cyber-arme ?

C’est bien connu, en matière de sécurité les risques ne proviennent pas seulement de l’extérieur du périmètre de l’entreprise mais bien de l’intérieur. Téléchargement de fichiers non autorisés, vol de données confidentielles ou encore accès à des informations par un collaborateur ayant quitté depuis des mois l’entreprise sont, malheureusement, une réalité qui dépasse – parfois – de loin la fiction. Et bien souvent, à la base de cette problématique, on trouve une gestion et/ou une politique de gestion des droits d’accès défaillante ou en tout cas plus en mesure de répondre à une évolution malsaine des comportements.
« Le constat que l’on fait aujourd’hui est que d’une façon générale la sécurité des accès et la configuration des droits d’accès pour accéder à des applications ou données sont souvent les parents pauvres de la sécurité informatique », explique Sébastien Faivre, co-fondateur de Brainwave. « En général, le département informatique et les métiers se renvoient la balle en termes de responsabilités dans les cas où on se rend compte que des personnes qui ont quitté l’entreprise ou changé de département ont toujours accès à des informations sensibles ou que d’autres encore ont des droits d’accès excessifs à des données critiques ».

Des jeux d’API couplés à des algorithmes d’analyse
Pour faire face à ce type de menace, le jeune éditeur francilien Brainwave (créé en 2010) a développé IdentityGRC qui permet de récupérer toutes les informations de configurations de l’ensemble des systèmes de l’entreprise afin de proposer une cartographie de l’ensemble des droits d’accès aux applications. Et ce, des systèmes CRM, ERP, gestion financière (SAP, Salesforce.com, Microsoft Dynamics CRM…) que des solutions cloud de sauvegarde et de partages documentaires (Google Drive, Dropbox…) ou encore des grands systèmes (AS400, RACF, CA Top Secret…). Pour y parvenir, plusieurs jeux d’API ont été développés, couplés à des algorithmes d’analyse, brevetés depuis fin 2010, afin de pouvoir poser des questions en langage naturel de type « Quelles sont les personnes ne faisant pas partie des ressources humaines qui ont accès aux fiches de paye des salariés ? ».
Aujourd’hui, Brainwave va plus loin en matière de détection mais surtout de prévention de la fraude et de fuite des données. « La version 2015 d’IdentityGRC propose de l’analyse comportementale permettant de mettre sous surveillance des comportements anormaux comme par exemple identifier une personne qui récupère bien plus de fichiers que ses collègues, mais également d’automatiser le diagnostic et la résolution des comportements suspects », fait savoir Sébastien Faivre. Une approche différente selon Brainwave des traditionnelles offres de sécurité centrées davantage sur les flux de comportements au niveau des postes de travail que sur le comportement du point de vue des applications, indépendamment du reste de tout terminal.

A partir de 75 000 euros la licence perpétuelle
Distingué par le Gartner dans la catégorie des « cool vendors » dans son rapport Magic Quadrant 2013 en Identity Analytics and Intelligence, Brainwave n’a pas attendu pareille reconnaissance pour se tailler une place dans les entreprises. Surtout les grandes, avec des clients comme PSA Peugeot-Citroën, Natixis, Crédit Agricole, BNP Paribas, ou encore Aéroports de Paris et Eutelsat qui utilisent ses solutions. En tout, l’éditeur revendique une cinquantaine de références en France mais également au Bénélux, en Suisse, au Royaume-Uni, au Magrehb ou encore au Canada où il a ouvert récemment un bureau commercial. Autofinancée jusqu’en 2014, la société a levé 2,5 millions d’euros fin 2014 afin de donner un nouvel élan à sa croissance internationale mais également renforcer ses équipes R&D (une dizaine de personnes sur 30 collaborateurs au total). Brainwave a réalisé l’année dernière un chiffre d’affaires de 2 millions d’euros et indique être rentable.
IdentityGRC 2015 est proposée à partir de 75 000 euros en licence perpétuelle, auquel vient s’ajouter près de 20 000 euros de maintenance annuelle. Deux modes de tarification sont proposées : nombre de personnes sur lequel un audit sécurité est réalisé ou bien en fonction du nombre d’applications. Quant à la disponibilité de l’offre, elle est pour le moment uniquement en on-premise. « Nous ne proposons pas d’offre en mode cloud public. Nos clients considèrent que ce type de données est sensible et préfèrent donc un déploiement sur site. Cependant, certains clients ont choisi un déploiement dans un cloud privé chez un infogéreur », explique Sébastien Faivre.

Source : http://www.lemondeinformatique.fr/actualites/lire-avec-identitygrc-2015-brainwave-s-ouvre-a-l-analyse-comportementale-61157.html
Par Dominique Filippone

Loi «Renseignement» : Ce que vous avez vu dans les séries TV pourrait bien se passer en vrai | Le Net Expert Informatique

	Loi «Renseignement» : Ce que vous avez vu dans les séries TV pourrait bien se passer en vrai

Quand la réalité rejoint la fiction. Le projet de loi renseignement, qui va être défendu par le gouvernement dans l'hémicycle du Sénat à partir de ce mardi, va « légaliser » certaines pratiques déjà utilisées par les services de renseignement. Les données récupérées avec ces nouveaux outils vont pouvoir être versées au dossier judiciaire des suspects.

Loi «Renseignement»: Les séries TV savent ce… *par 20Minutes*

Si elle fait l'objet d'un large consensus parmi la majorité des parlementaires, cette loi est contestée par les sénateurs communistes qui ont déposé une série d'amendements de suppression et ont dénoncé un risque de « surveillance de masse ». La plupart des techniques sur le point d'être légalisées sont déjà utilisées. Et diffusées dans les séries TV. Florilège…

Poser un mouchard sous une voiture
Dans Breaking Bad (Episode 9, Saison 5), Walt accuse Hank qui travaille pour la DEA, la brigade des stupéfiants américaine, d'avoir posé un tracker GPS sous sa voiture. Le projet de loi prévoit l'emploi de balises « permettant de localiser en temps réel un véhicule ou un objet ».

Mettre un appartement sous vidéosurveillance

Dans la deuxième saison de Scandal, l'appartement de l'avocate Olivia Pope est placé sous vidéo-surveillance par Jake Ballard, le fidèle ami du président. Elle s'en rend compte dans le 18e épisode. Des caméras partout, ainsi que des micros quasiment indétectables sont utilisés. Le projet de loi permettra aux services de renseignement d'appliquer ce type d'écoutes. Les policiers passeront cependant à travers le filtre de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Les plus sceptiques regrettent le pouvoir amoindri de cet organe de contrôle.

Géolocaliser un téléphone portable

Dès le premier épisode de la saison 1 du Bureau des Légendes, Cyclone, un des clandestins du BDL, est arrêté à Alger alors qu'il est ivre au volant d'une voiture. Le Bureau des Légendes va s'inquiéter : Cyclone étant musulman pratiquant, il n'aurait pas dû être saoul. Sisteron décide alors de géolocaliser son téléphone portable. Le signal du mobile indique qu'il se trouve bien au commissariat.

Intercepter les métadonnées d'un téléphone
Dans la série américaine Those who kill, Catherine Jensen, experte en tueurs en série, fait appel à un détective de la brigade des stupéfiants pour mettre sur écoute un suspect. Ce dernier, à l'épisode 9 détaille comment les policiers parviennent à récupérer les données enregistrées sur un téléphone portable, en se faisant passer pour une antenne relais après avoir copié la carte sim. Dans la « vraie vie », les policiers utilisent des Imsi-Catchers qui peuvent intercepter dans un rayon donné toutes les données qui transitent via un téléphone. Cette technologie, rendue possible par la loi renseignement, fait pourtant polémique.

Capter un écran d'ordinateur en direct grâce à un logiciel espion
Les experts de CSI : Cyber (saison 1, épisode 1), mettent au point ce qu'ils appellent un RAT (Remote Administration Tool), un outil d'administration à distance. En clair, un programme permettant la prise de contrôle total, à distance, d'un ordinateur depuis un autre ordinateur. Ils y ont introduit un logiciel espion qui permet, en fonction de mots-clés utilisés dans un mail, d'activer une alarme. Ils peuvent aussi capter en direct le mot-clé qui est tapé. Les défenseurs de la liberté numérique dénoncent à travers la loi Renseignement la surveillance massive des ordinateurs des internautes.

Source : http://www.20minutes.fr/societe/1621371-20150602-video-loi-renseignement-vu-series-tv-ca-pourra-passer-vrai
Par William Molinié

Les cyber-attaques changent de forme…| Le Net Expert Informatique

	Les cyber-attaques changent de forme…

Akamai constate une évolution du profil des attaques informatiques par déni de service distribué (DDoS), mais aussi des assauts contre les services Web.

Le profil des attaques informatiques par déni de service distribué (DDoS, visant à rendre des ressources indisponibles en les saturant de requêtes) a fortement évolué en un an, tandis que de nouvelles menaces sont nées de l'adoption du protocole IPv6.
Telles sont les principales conclusions émises par Akamai dans la dernière édition de son baromètre Internet Security – document PDF, 93 pages – portant sur le 1er trimestre 2015.
Sur le volet DDoS, le constat est sans appel : les assauts se multiplient (+ 116,5 % d'une année sur l'autre). Les attaques sur la couche applicative (Layer 7) augmentent de 60 %, mais ne représentent encore qu'un cas sur dix.
Le reste des offensives se concentre sur l'infrastructure (Layers 3 & 4 ; + 125 %), qui permet de maximiser plus facilement la puissance des attaques tout en nécessitant moins de ressources.
Alors qu'un DDoS s'échelonnait en moyenne sur 17 heures au 1er trimestre 2014, la durée a avoisiné les 25 heures un an plus tard (+ 43 %). Des attaques plus longues, donc, mais aussi moins virulentes : 5,95 Gbit/s de bande passante moyenne, contre 9,7 Gbit/s un an plus tôt ; quant au nombre moyen de paquets envoyés par seconde, il baisse de 89 % (2,21 millions).
Akamai a tout de même relevé 8 attaques d'un volume supérieur à 100 Gbit/s.
Encore quasiment inexploité début 2014, le SSDP (« Simple Service Discovery Protocol ») est devenu, en l'espace d'un an, le principal facteur déclencheur des attaques DDoS (plus d'un cas sur cinq). Implémenté et activé par défaut sur des millions d'équipements (routeurs, webcams, imprimantes, TV connectées) pour leur permettre d'interagir sur un réseau local, ce protocole est souvent mal – ou pas du tout – sécurisé.
L'industrie du jeu vidéo concentre à elle seule 35 % des dénis de services répertoriés entre le 1er janvier et le 31 mars. Suivent le secteur IT (25 %), les télécoms (14 %), la finance (8,4 %), les médias (7,5 %), l'éducation (5 %), la distribution (2,3 %) et le secteur public (2 %).
Pour la première fois, Akamai inclut dans son baromètre les attaques contre les applications Web. Les analyses réalisées sur environ 180 millions d'échantillons ont permis de dégager 7 vecteurs de piratage.
Dans les deux tiers des cas, les cybercriminels ont exploité une faille de type LFI (« Local File Inclusion ») leur permettant d'accéder, en lecture, à des fichiers hébergés sur un serveur Web. On notera cette campagne massive venue d'Allemagne contre deux grands noms du secteur de la distribution via une vulnérabilité dans le plugin WordPress RevSlider.

SQL, HTTPS et IPv6
29 % des attaques recensées sont liées à des injections SQL* ; c'est-à-dire à l'exploitation d'une brèche dans une application qui interagit avec une base de données en introduisant une requête SQL non prévue par le système. Illustration avec cette campagne issue essentiellement d'Irlande et visant une société de l'industrie du voyage.
Les autres types d'attaques (inclusion de fichiers distants sur des serveurs Web, injection de code PHP, exécution de commandes shell sur le système visé…) n'ont été repérées que dans environ 5 % des cas. Sachant toutefois qu'au global, près de 10 % ont été menées sur des sites « sécurisés » en HTTPS…
Parmi les grandes tendances de l'année, Akamai pointe la menace grandissante des sites dits « booters » ou « stressers » et qui permettent de simuler des attaques DDoS. Alors qu'il y a encore un an, leur ampleur se limitait à 10 ou 20 Gbit/s, ils peuvent désormais lancer des assauts dévastateurs à plus de 100 Gbit/s, en exploitant notamment des techniques de réflexion du trafic.
Autre enjeu à surveiller : l'adoption du protocole IPv6, qui permet d'élargir l'espace d'adressage réseau… mais dont l'architecture est dite « imparfaite » par Akamai : il est possible de passer outre certaines protections implémentées dans IPv4. Il existe d'ailleurs « plusieurs signes » montrant que les cybercriminels mènent bien des recherches sur le sujet.
* Documentées depuis 1998, les attaques par injection SQL vont désormais bien au-delà du simple vol de données. Elles permettent aussi l'élévation de privilèges, l'exécution de commande, la corruption de systèmes…

Source : http://www.itespresso.fr/securite-it-cyber-attaques-changent-forme-97172.html

Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails | Le Net Expert Informatique

	Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails

Peut-on se passer de l'e mail dans le cadre de ses activités professionnelles ? Pratique et instantanée, la communication par e-mail s'est imposée au quotidien dans l'entreprise. Certaines études évaluent à plus de 100 milliards le nombre d'e-mails professionnels qui sont échangés chaque jour(1).

Nos e mails risquent-ils de laisser échapper des données sécurisées ?
Malgré ses nombreux atouts, l'e-mail présente également certains risques. Des récits de fuites de données sensibles font régulièrement la une des médias. Un des derniers incidents en date : la récente divulgation des numéros de passeport de 31 leaders mondiaux. En cause ? La fonctionnalité de saisie automatique à partir du carnet d'adresses d'Outlook. Cette fonctionnalité – aussi pratique soit-elle – ne fait qu'accentuer le risque de diffuser, par erreur, des données confidentielles.
Malgré l'augmentation du nombre d'erreurs d'aiguillage d'e-mails et l'évolution du contexte législatif – comme en atteste la récente loi australienne sur l'obligation de conserver des métadonnées et d'autres textes réglementant la transmission de données confidentielles (HIPAA, FIPPA et PCI) –, on peut s'étonner que les entreprises ne soient pas plus nombreuses à choisir de sécuriser le contenu de leurs e mails.
L'e mail est sans doute un peu trop pratique à en juger par la facilité avec laquelle des informations sensibles peuvent être envoyées, au risque de tomber dans les mauvaises mains.

Quelques chiffres :
• 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes (2).
• 21 % des employés déclarent envoyer des données sensibles sans les chiffrer(2). Les coûts liés à la perte de données s'envolent, sans parler des conséquences sur la réputation des entreprises et des éventuelles répercussions sur le plan juridique en cas de violation de la réglementation sur la transmission et le stockage de données confidentielles (notamment dans le cadre des lois HIPAA et FIPPA, et du standard PCI).
• 22 % des entreprises sont concernées chaque année par la perte de données via e-mail(3).
• 3,5 millions de dollars : coût moyen d'une violation de données pour une entreprise(4).

La solution
Il existe heureusement des solutions de sécurité des e-mails qui mettent les utilisateurs et leur entreprise à l'abri de ces menaces. La signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message et évitent que des données sensibles ne tombent dans de mauvaises mains. Le destinataire a également l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
Le chiffrement d'un e-mail revient à sceller son message puis à le déposer dans un dossier verrouillé dont seul le destinataire prévu possède la clé. Il est alors impossible pour une personne interceptant le message, pendant son transit ou à son emplacement de stockage sur le serveur, d'en voir le contenu. Sur le plan de la sécurité, le chiffrement des e mails présente les avantages suivants :
• Confidentialité : le processus de chiffrement requiert des informations de la part du destinataire prévu, qui est le seul à pouvoir consulter le contenu déchiffré.
• Intégrité du message : une partie du processus de déchiffrement consiste à vérifier que le contenu du message d'origine chiffré correspond au nouvel e-mail déchiffré. Le moindre changement apporté au message d'origine ferait échouer le processus de déchiffrement.
Avant de choisir une solution, il est important d'avoir en tête plusieurs choses. L'utilisateur est le mieux placé, car il connaît son entreprise mieux que personne. Phishing, perte de données… quels sont ses principaux sujets de préoccupation ? Quelle est l'infrastructure de messagerie en place dans l'entreprise ? Quel est le cadre réglementaire ? Les réponses propres à chaque entreprise orienteront les choix vers la solution la plus appropriée.

Sources :
(1) Email Statistics Report 2013-2017, The Radicati Group, Inc.
(2) SilverSky Email Security Habits Survey Report, SilverSky, 2013
(3) Best Practices in Email, Web, and Social Media Security, Osterman Research, Inc., January 2014
(4) Global Cost of Data Breach St'sudy, Ponemon Institute,

Source : http://www.globalsecuritymag.fr/Les-dernieres-fuites-de-donnees,20150601,53078.html
par GlobalSign

Protection des données personnelles : les entreprises bel et bien contraintes | Le Net Expert Informatique

	Protection des données personnelles : les entreprises bel et bien contraintes

Pensée pour protéger le citoyen, la loi Informatique et libertés est de plus en plus détournée de son objectif premier. Tant par les salariés que par les entreprises elles-mêmes, qui n'hésitent plus à s'en servir comme arme concurrentielle. L'analyse de l'avocat François Coupez.

La protection des données à caractère personnel est née en France avec la loi du 6 janvier 1978 dite « Informatique et libertés ». Le texte a été modifié en 2004 (à la suite de la directive européenne 95/46), et il est destiné à l'être à nouveau par le projet de loi sur le numérique annoncé en grande pompe depuis deux ans maintenant… avant d'être de toute façon complètement remplacé par un projet de règlement européen (http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do%3Freference=2012/0011(COD)%26l=fr) encore en discussion qui unifiera en 2017 ou 2018 le droit de tous les pays de l'Union européenne sur le sujet.

Si ces différents projets visent à accroître de façon très importante les sanctions financières, ils ont également pour but de permettre une application plus efficace des règles (droit à l'oubli numérique/au déréférencement, co-responsabilité des sous-traitants, etc.). Mais en parallèle, on constate depuis quelques années le développement d'une véritable instrumentalisation de cette protection légale, aux règles extrêmement formelles et aux impacts potentiellement dévastateurs[1] sur l'image des entreprises prises en faute.

Salariés et clients, quand le pouvoir change de camp

Historiquement, la CNIL a eu l'occasion d'appliquer les principes de la loi « Informatique et libertés » dans plusieurs domaines, avec la plupart du temps deux points communs : d'une part la protection des clients contre l'utilisation qui serait faite de leurs données en contradiction avec les règles applicables et, d'autre part, la protection des salariés dans des hypothèses de surveillance abusive, de discrimination ou de mode d'évaluation des performances illicites.
Dans les deux cas, l'action de la CNIL conduit souvent l'entreprise fautive à revoir beaucoup plus globalement l'ensemble de ses processus et leur conformité.
Or les difficultés pratiques concernant le respect de cette réglementation pour l'entreprise ne doivent pas être sous-estimées. Elles tiennent tant à son formalisme qu'à ses conditions d'application, étant entendu que les traitements de ce type de données se développent de façon exponentielle avec la transformation numérique. De plus, l'entreprise, confrontée à un lacis réglementaire croissant et dans tous les domaines, alloue parfois ses ressources pour se mettre en conformité en fonction de l'urgence, ou du risque réel de sanction. Les entreprises ne peuvent ainsi pas toujours prétendre réussir un sans-faute en matière de protection des données personnelles… et en sont pleinement conscientes.
En parallèle, un phénomène se développe depuis quelques années, à un point tel qu'il se généralise. Sentant la faille, des clients ou des salariés bien informés n'hésitent plus à l'utiliser, non pour faire valoir leurs droits en la matière, mais pour faire pression dans le cadre d'un contentieux ou d'une revendication autre. La réglementation devient alors un simple prétexte destiné à faire plier son opposant.
Concernant le cas des clients, cela concerne souvent les entreprises disposant de nombreux points de contact avec la clientèle (et disposant de nombreux conseillers clientèles, etc.). Dans les grands réseaux, il est toujours plus difficile de faire respecter à tous les salariés en contact avec la clientèle les règles de base (notamment concernant la zone de « bloc-note » ou de note en champ libre sur les fiches clients, propices à tous les excès), ce qui multiplie les hypothèses de manquements ;
Quant aux salariés, il est de plus en plus fréquent qu'ils fassent jouer leurs droits en la matière. Par exemple, l'une des pratiques les plus fréquentes est de systématiquement avoir recours au droit d'accès aux données personnelles que leur employeur collecte sur eux, lorsque le contrat de travail arrive précocement à son terme, ou que les deux parties se retrouvent aux Prud'hommes. La pratique montre ainsi que, sur l'ensemble des personnes pouvant faire valoir leur droit d'accès dans le cas de traitements réalisés par une entreprise, près de 75% des demandes proviennent de l'interne et donc des salariés. Ainsi, il n'y a qu'à regarder la jurisprudence en droit social ces dernières années pour s'apercevoir qu'il est devenu aussi courant d'alléguer un traitement de données personnelles contraire à la loi, et donc de l'illicéité du moyen de preuve opposé à un salarié, que d'en appeler aux pages Facebook en matière de divorce. Un exemple récent nous vient de l'arrêt de la Cour d'appel de Rouen rendu le 12 mai 2015 qui invalide les preuves concernant d'une part un système de badgeage (pas d'information du comité d'entreprise) et d'autre part un logiciel permettant de contrôler les horaires des salariés (pas de formalités CNIL) : le licenciement est ainsi considéré comme étant sans cause réelle ni sérieuse.

Maintenant les contentieux… entre entreprises ?

Ce qui est plus marquant encore, c'est que ce phénomène est en passe de gagner les relations entre entreprises.
Alors que l'on s'attend à ce que ce soit la victime (client, salarié, etc.) qui fasse valoir les droits qui lui sont reconnus, les tribunaux sont en effet saisis de façon croissante de manquements à cette réglementation allégués par… des sociétés concurrentes.
Pour mettre fin à un partenariat commercial, annuler une vente, tenter de prouver une rupture abusive des relations commerciales ou empêcher un concurrent de commercialiser un service innovant, les hypothèses se multiplient dans lesquelles des tribunaux de tout type sont confrontés à cette situation.

En voici quelques exemples :

le 25 juin 2013, la Cour de cassation a rendu une décision conduisant à l'annulation de la vente d'un fichier de clients informatisé. Dans cette affaire, les associés d'une entreprise avaient vendu pour 46 000 € le seul fichier des clients de l'entreprise, fort de 6 000 clients référencés depuis 1946. Or pour l'acheteur ayant utilisé quelques semaines cette base, celle-ci était une coquille vide de 1 950 clients actifs seulement. Il en demandait donc le remboursement… qu'il obtint : pour la Cour de cassation, l'absence du respect des formalités CNIL rend toute commercialisation du fichier impossible, la vente ayant nécessairement un objet illicite.
À la suite d'une décision de la CNIL du 8 septembre 2011 autorisant pour la première fois une entreprise à traiter pour des raisons commerciales le numéro NIR (aussi appelé « numéro de sécurité sociale »), une entreprise concurrente a formé un recours considérant que l'interprétation était contestable au sens de la loi Informatique et libertés et qu'elle conduisait à un avantage concurrentiel injustifié. C'était le premier recours intenté à l'encontre d'une décision d'autorisation, alors qu'en général – et logiquement – les recours sont formés en cas de refus de la CNIL. Or, le Conseil d'État, s'il a confirmé la décision de la CNIL le 26 mai 2014, a surtout reconnu le droit à agir de la société concurrente dans cette affaire (voir, à ce sujet, l'excellent article de Guillaume Desgens-Pasanau dans Expertises N° 397 de Décembre 2014: « Données personnelles : ouverture de l'usage du NIR au secteur privé »).
Dans une affaire récente de rupture abusive alléguée de relations commerciales, la société se plaignant de la rupture (société B) proposait à l'autre société (A) de numériser pour elle des documents dans lesquels figuraient des données personnelles, et d'effectuer cette prestation depuis le Vietnam. La société A aurait donc dû demander l'autorisation de la CNIL du fait des flux de données vers ce pays, ce qu'elle n'a pas fait. Inaction qui, pour la société B, constitue un élément de preuve que la société A ne croyait en réalité pas au projet et ne comptait pas sérieusement contracter avec elle. La Cour d'appel de Paris toutefois, pour des raisons de défaut de preuve, n'a pas suivi cette analyse et a considéré le 10 avril 2015 qu'il n'y avait pas de rupture abusive.

Le grand classique des contentieux de demain ?

On le voit à travers ces quelques exemples jurisprudentiels récents, le phénomène va croissant. Il est surtout appelé à prendre encore de l'ampleur avec le futur projet de règlement européen, qui conduit à remplacer les formalités préalables par un contrôle constant de conformité et oblige donc à documenter la façon dont les traitements sont opérés à toutes les étapes. Or toutes ces informations forment un vivier de preuves de ce qui a été fait (ou pas), destinées au régulateur… et qui pourraient facilement être utilisées par une société concurrente dans le cadre d'un procès.
Plus globalement, les entreprises doivent prendre conscience de cette évolution et en saisir toutes les opportunités, mais également tous les risques : il semble logique que les études de risque, réalisées préalablement à la mise en œuvre de traitement de données à caractère personnel, aient également à prendre en compte cette nouvelle donne…

A terme en effet, en cas de contentieux et dès que l'on parlera de près ou de loin de données, la vérification de la licéité des traitements de données personnelles de l'entreprise adverse pourrait devenir un préalable aussi convenu que la vérification des pouvoirs du signataire d'un acte.

Si cette évolution peut paraître critiquable car compliquant encore les dossiers en justice, elle est malgré tout le signe que la réglementation sur les données personnelles s'ancre profondément dans les habitudes. Un réel progrès, et qui n'était pas chose évidente il y a encore quelques années…

[1] Certes, 17 textes pénaux prévoient une sanction de 5 ans d'emprisonnement et de 1 500 000 € d'amende pour les entreprises qui enfreindraient les règles en la matière, mais les applications jurisprudentielles sont rarissimes. Les sanctions de la CNIL sont quant à elles beaucoup plus fréquentes, avec des montants financiers pour le moment limités à 150 000 € (le double en cas de récidive), seul Google inc. ayant été condamné à une telle peine. Leur efficacité est fortement renforcée par leur publication (fort effet d'image sur les grandes entreprises).

Source : http://www.silicon.fr/protection-donnees-personnelles-loi-instrumentalisee-116895.html
Par François Coupez, Avocat à la Cour, Associé du cabinet ATIPIC Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies

---

L'employé, la première faille de sécurité | Le Net Expert Informatique

L'employé, la première faille de sécurité

Si les entreprises se concentrent toujours sur leur protection informatique vis-à-vis des intrusions externes, se méfient-elles assez de leurs propres employés ? Pas toujours à en croire certaines histoires de ces dernières années.

L'ennemi a beau souvent être à l'extérieur de l'entreprise, il n'en reste pas moins que les employés eux-mêmes peuvent devenir de véritables problèmes, à plus ou moins grande échelle. Bien entendu, les plus grands risques internes sont faits à l'insu du collaborateur, du fait de son manque de technique et/ou d'attention, mais parfois, l'acte malveillant est réellement sciemment.

L'affaire Coca Cola

Fin 2013, le géant Coca Cola, qui compte tout de même près de 130 000 employés, s'est par exemple rendu compte qu'elle avait été victime durant de longues années d'un voleur d'ordinateurs portables. L'employé en question a ainsi dérobé 55 ordinateurs sur plusieurs années, volant ainsi des données sur environ 74 000 personnes, la plupart étant des employés du géant américain ou des collaborateurs reliés à la firme.

Réalisé par un employé (au nom inconnu) ayant en charge les équipements informatiques, non seulement l'acte en lui-même a sonné comme une véritable claque pour la firme US, mais surtout, parmi toutes les données concernées, 18 000 concernaient les numéros de sécurité sociale, données particulièrement sensibles outre-Atlantique.

Pire encore, selon un mémo de Coca Cola envoyé aux employés et révélé par le Wall Street Journal, aucune des données volées n'était chiffrée. Nous apprenons aussi qu'afin d'éviter la panique, le spécialiste de la boisson gazeuse a tenté de résoudre le problème en secret durant plusieurs semaines. Les vols ont ainsi été remarqués en décembre 2013, mais la firme a attendu le 24 janvier pour en informer ses employés.

Plus que le côté technique, cette histoire nous montre donc que la sécurité est aussi (surtout ?) une question de processus. La « faille » de Coca Cola ainsi été humaine et organisationnelle plus qu'autre chose.

Boeing aussi

Coca n'est toutefois pas la seule très grande compagnie concernée par ce genre de problématique. En 2006, un employé de Boeing a par exemple été licencié non pas pour avoir dérobé du matériel et des données, mais du fait de sa responsabilité dans un vol d'ordinateur. Le collaborateur a ainsi enfreint les règles de l'entreprise en téléchargeant des informations confidentielles sur son PC portable sans même les chiffrer.

Problème, l'employé avait téléchargé des données personnelles de 380 000 employés actuels et passés de la compagnie, comme des numéros de sécurité sociale, des noms, des adresses, etc. Le tout fut ensuite volé en décembre 2006, entraînant le licenciement du collaborateur.

Cette faute grave n'était pas une première, puisque selon le porte-parole de Boeing, deux autres vols d'ordinateurs portables contenant des données sur les employés ont été dérobés entre 2005 et 2006. « Nous encourageons les gens à travailler hors du serveur, ce qui permettrait de garder l'information derrière le pare-feu. Si vous téléchargez des informations sur votre ordinateur portable, cela est censé être temporaire et l'information est censée être cryptée » a bien insisté Boeing à l'époque. Du simple bon sens a priori peu respecté par certains de ses employés.

Moralité de ces deux histoires : la sécurité est avant tout une affaire d'organisation, de processus et de règles. S'il est évident qu'il faut se prémunir des actions malintentionnées extérieures, « l'ennemi » peut aussi être à l'intérieur, que ce soit du fait d'actes réalisés délibérément ou non. BYOD ou non, les comportements des employés peuvent être cruciaux pour la sécurité de l'entreprise. Rédiger une politique stricte et mettre en place des systèmes de surveillances (ou au moins de vérification), notamment pour ceux manipulant des données sensibles, est ainsi indispensable si l'on veut éviter de lourdes déconvenues…

Source : http://www.zdnet.fr/actualites/l-employe-la-premiere-faille-de-securite-39819662.htm

Protection des données. Un accord européen possible le 15 juin | Le Net Expert Informatique

Un accord pour adapter la législation européenne sur la protection des données personnelles à l'essor de l'internet est à portée de main et peut être conclu le 15 juin.

Jeudi soir à Bruxelles, l'Allemagne, la France, le Luxembourg et la Commision européenne ont assuré qu'un accord sur la protection des données pourrait voir le jour d'ici à trois semaines.
« Nous sommes dans la dernière ligne droite et nous voulons aboutir », a déclaré le ministre allemand de l'Intérieur, Thomas de Maizière, au cours d'un débat sur la protection des données avec les ministres de la Justice de la France, du Luxembourg et la commissaire européenne Vera Jourova.
« Nous sommes sur la voie d'un accord général. Le texte est inachevé, mais il est bon », a confirmé Mme Taubira. « Nous avons en perspective un accord le 15 juin » lors de la réunion des ministres européens de la Justice à Luxembourg, a renchéri la commissaire Jourova.

Protéger les citoyens européens

L'objectif de cette nouvelle législation est d'empêcher les données personnelles des citoyens de l'UE de quitter l'espace européen sans leur consentement explicite.
Thomas de Maizière a préconisé une longue journée de discussion pour aboutir. « Il va falloir faire des compromis et tempérer les attentes », a-t-il insisté.
Deux textes sont en discussion depuis février 2012: un règlement pour les données personnelles à caractère civil et commercial, et une loi pour les fichiers du secteur privé.

Source : http://www.ouest-france.fr/un-accord-europeen-possible-le-15-juin-3436970