Surveillance des salariés et logiciel de détection d’infractions pédopornographique | Le Net Expert Informatique

Surveillance des salariés et logiciel de détection d’infractions pédopornographique

Dans un arrêt du 11 mai 2015, le Conseil d’État confirme une délibération de la Cnil refusant à une entreprise la mise en place sur les postes informatiques d’un logiciel de recherche des infractions à caractère pédopornographique.

Si l’employeur peut exercer une surveillance sur les connexions internet des salariés sur leur poste de travail, de là à pouvoir mettre en œuvre un logiciel ayant pour objet de collecter des données relatives à la consultation par les salariés de sites à caractère pédopornographique, il y a un pas que n’a pas franchi la Cnil ni le Conseil d’État.
En effet, le Conseil d’État a été saisi par une entreprise d’une demande d’annulation de la décision de la Cnil lui refusant l’autorisation de mettre en place un tel logiciel.
La Haut juridiction n’a pas annulé la décision de la Cnil en considérant que la loi informatique et libertés ne permet à une entreprise privée de mettre en œuvre un traitement de données personnelles visant des infractions pénales ou qui peuvent en établir l’existence.

CE 11 mai 2015, n° 375669
Lire la suite….

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

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

Source : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126327/Surveillance-des-salaries-et-logiciel-de-detection-dinfractions-pedopornographique.aspx
Par Dominique Jullien

Alerte ! Des images informatiques infectées, le nouveau danger… | Le Net Expert Informatique

Alerte ! Des images informatiques infectées, le nouveau danger…

Lors de la conférence Hack In The Box d'Amsterdam, un chercheur en sécurité informatique présente Stegosploit, un outil qui permet de cacher un code malveillant dans une image.

Imaginez, vous êtes en train de surfer quand soudain votre machine devient folle ! Un code malveillant vient d'être installé alors que vous avez un antivirus et vos logiciels à jour. Une image, affichait par un site que vous veniez de visiter vient de lancer l'attaque. De la science-fiction ? Pas avec les preuves de Saumil Shah, un chercheur en sécurité informatique.
L'ingénieur a expliqué lors de la conférence (HiP) Hack In The Box que des pirates étaient très certainement en train d'exploiter sa découverte. L'idée, cacher un code malveillant dans une image en utilisant la stéganographie (cacher une information dans un autre document, NDR). Des recherches de Shah est sorti Stegosploit, un logiciel qui code en Javascript un logiciel malveillant dans les pixels d'une image au format JPEG ou PNG.

Source : http://www.datasecuritybreach.fr/stegosploit-loutil-qui-cache-un-code-malveillant-dans-une-image/#axzz3cN0qvWLQ

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

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

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

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.

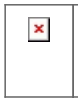
Problème, l'employé avait téléchargé des données personnelles de 380 000 employés actuels et passés de la compagnie, comme des numéros de sécurité sociale, des noms, des adresses, etc. Le tout fut ensuite volé en décembre 2006, entraînant le licenciement du collaborateur.

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

La voiture autonome vulnérable aux cyber-attaques, selon des experts | Le Net Expert Informatique



La voiture autonome vulnérable aux cyber-attaques, selon des experts

Le risque de voir des pirates informatiques prendre le contrôle de voitures autonomes est bien réel, estiment des experts américains, une hypothèse d'ores et déjà prise en compte par les constructeurs et les assureurs aux Etats-Unis.

Annoncées sur les routes en 2020, voire même dès 2017, la voiture sans conducteur devrait disposer des technologies dernier cri comme des capteurs numériques –caméras, radars, sonars, lidars (guidage par laser)– gérées à distance par des logiciels permettant de reconnaître des limites de chaussées, des panneaux ou encore des obstacles.
Mais, comme pour les automobiles connectées et leurs systèmes multimédias embarqués, ces nouvelles technologies de pointe censées rendre les véhicules plus sûrs et fiables, pourraient aussi les rendre vulnérables aux attaques de hackers, selon les sociétés de sécurité informatique américaines Mission Secure Inc (MSi) et Perrone Robotics Inc.
Un pirate informatique s'est récemment vanté d'avoir pénétré les systèmes électroniques d'un avion de ligne dans lequel il voyageait, et d'en avoir modifié la trajectoire. Ceci en utilisant le système wifi proposé aux passagers.
Les deux sociétés de sécurité ont effectué, en collaboration avec l'Université de Virginie (est) et le ministère américain de la Défense, des tests en situation réelle qui ont montré, selon elles, qu'il était possible de désorganiser le système.
L'un des essais consistait à modifier le comportement de la voiture face à un obstacle: le piratage «oblige la voiture à accélérer au lieu de freiner même si l'obstacle a été détecté par le Lidar, entraînant une collision à grande vitesse», selon le rapport consultable sur le site internet de MSi (missionsecure.net).
Une autre cyber-attaque «provoque un freinage d'urgence inapproprié plutôt qu'un freinage en douceur, pouvant entraîner la perte de contrôle du véhicule», peut-on encore lire.
Selon ces experts, les pirates pénètrent le système grâce aux connexions sans fil, bluetooth et wifi.
MSi et Perrone Robotics, qui développent un système payant pour parer les cyber-attaques, estiment que «cette situation pose des défis importants et des risques pour l'industrie automobile ainsi que pour la sécurité publique».
– Primes d'assurances revues ? –
La plupart des constructeurs automobile s'attelant à la fabrication de leur voiture autonome n'ont pas donné suite aux sollicitations de l'AFP sur le sujet.
Mais, selon des sources proches de l'industrie, les éventualités de cyber-attaques ont été prises en compte et testées tout au long du processus de fabrication.
Le géant de l'internet Google, par exemple, aurait une équipe d'informaticiens de haut vol chargée de défier les logiciels destinés à sa propre voiture autonome qui va être testée sur la voie publique à partir de cet été, selon des sources industrielles.
Contacté par l'AFP, le groupe de Mountain View (Californie) s'est refusé à tout commentaire.
Cette question de sécurité préoccupe les assureurs américains qui sont dans l'expectative face à ces nouvelles technologies et à leur capacité à réduire réellement les risques d'accidents. Cela pourrait les obliger à repenser leurs contrats et à recalculer les primes.
Dans un premier temps, ces dernières pourraient augmenter à cause du prix des voitures autonomes, qui sera élevé en raison du coût des technologies embarquées et des réparations éventuelles, a expliqué l'assureur Nationwide à l'AFP.
Mais, a-t-il ajouté, cela pourrait être en partie compensé avec la généralisation de ces véhicules supposés éviter les accidents. Pour State Farm, autre assureur américain, il est nécessaire d'avoir une «vue d'ensemble».
«Certes les technologies des voitures autonomes et connectées réduisent ou éliminent certains risques auxquels font face aujourd'hui les conducteurs, mais de nouveaux risques vont probablement apparaître», a argumenté la compagnie.
Selon un important assureur américain ayant requis l'anonymat, il sera essentiel de bien baliser les responsabilités en cas d'accidents. Celles-ci seront établies en fonction des instructions des constructeurs automobiles sur ce que la voiture pourra faire ou non de manière autonome.

Source : http://www.liberation.fr/economie/2015/05/31/la-voiture-autonome-vulnerable-aux-cyber-attaques-selon-des-experts_1320239

| Le Net Expert Informatique