Comment se protéger du virus Dridex contenu dans les e-mails piégés | Denis JACOPINI

Comment se protéger du virus Dridex contenu dans les e-mails piégés

Après un mois d'interruption seulement, l'un des logiciels malveillants les plus virulents de 2015 fait son retour en France : plusieurs vagues d'envois massifs de courriels contenant le virus Dridex ont été constatées ces derniers jours. Ce malware de type « cheval de Troie » s'installe sur les ordinateurs Windows par le biais de pièces jointes piégées, dans le but de voler des coordonnées bancaires.

D'où vient ce virus ?

Identifié dès juillet 2014 et repéré dans au moins 26 pays, Dridex n'a jamais vraiment disparu. Pourtant, fin août, une opération internationale coordonnée par le FBI et Europol (E3C), les agences de sécurité américaine et européenne, aboutissait à l'arrestation du Moldave Andreï Ghinkul, dit « Smilex », principal administrateur du virus. Les envois des courriels non-sollicités avaient été stoppés presque totalement le 2 septembre.

Mais le soulagement a été de courte durée : le 1er octobre, Palo Alto Networks détecte une nouvelle activité de Dridex au Royaume-Uni, puis le 14 octobre, c'est au tour de l'éditeur d'antivirus Avira d'émettre des doutes sur l'arrêt réel du botnet (réseau de serveurs et programmes destinés à propager le virus). Ce dernier paraît en effet toujours actif, selon Ayoub Faouzi, l'un des experts d'Avira.

Et effectivement, en France, le CERT-FR avertit le 23 octobre qu'une soixantaine de vagues d'envois massifs d'e-mails piégés visant la France ont eu lieu en moins de quinze jours.

Une nouvelle technique d'assemblage du code dite « just-in-time » (ou à la volée) permet aux pirates d'éviter les détections, mais aussi d'adapter plus rapidement le malware – une technique utilisée par d'autres logiciels malveillants comme GameOver Zeus.

Comment fonctionne t-il ?

Le mail reçu se présente de façon anodine : la plupart du temps, une relance de facture, incluant une pièce jointe au format. doc de Microsoft Office. À l'heure actuelle, peu d'antivirus détectent la nouvelle variante de ce logiciel (qui est signé avec un certificat officiel paraissant émaner de l'entreprise de sécurité Comodo), et la plupart ne suppriment donc pas la pièce jointe.

Si le destinataire tente d'ouvrir le document Word joint, une page vierge va s'afficher, mais le logiciel de Microsoft va tout de même demander à l'utilisateur s'il veut activer les macros (permettant d'interpréter les codes éventuellement contenus dans les documents Office). Une réponse positive active le virus et va lancer le téléchargement discret d'un premier code malicieux.

D'autres fichiers sont ensuite téléchargés afin d'installer divers programmes-espions. Il ne reste plus au pirate qu'à décider quand et quel programme utiliser et installer pour récupérer les données personnelles et bancaires puis effectuer des opérations frauduleuses.

A quoi ressemblent ces e-mails piégés ?

Les premières vagues de mails, le plus souvent intitulés « Relance Facture urgent » ou de « AR CDE + Facture Proforma », ont touché des messageries personnelles ou d'entreprises dès le mois de juin. Ecrits dans un français très correct et sans fautes d'orthographe, ces textes courts, et suffisamment sibyllins pour inquiéter ceux qui les reçoivent, ont déjà fait l'objet d'une première alerte officielle émanant du CERT-FR, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. La nouvelle vague de mails reçus ces deux dernières semaines sont du même tonneau.

Exemples :

« Objet : PIXOLUTIONS – FACTURE N°03480830-260615

Bonsoir,

Veuillez trouver en pièce jointe la facture n°03480830-260615 correspondant à la réalisation et pose du logo végétalisé à Perpignan. Vous en souhaitant bonne réception, bien cordialement, ».

« Objet : DUPLICATA FAC N°87878241

Salut,

Il parait que tu recherches la facture avec les Rimauresq Rosé et Blanc ? La voici en pièce jointe. Veux-tu que je te la remette au courrier également ? »

« Objet : Comptabilité de PACAR : facture n° 94352132 du 26/10 de 439,99 euros

Bonjour,

Pouvez-vous nous envoyer un chèque de 439,99 euros en paiement de la facture n° 94352132 dont vous trouverez la copie ci-jointe. En vous remerciant, Bien cordialement, »

Comment s'en protéger ?

En plus d'un antivirus à jour, il est recommandé d'observer une grande vigilance à la réception de tout message contenant une pièce jointe, et ce quel que soit son format (.doc, .odt, .xls, .pdf, etc.).

Si le courriel semble émaner d'un organisme officiel (administrations, banques, boutiques en ligne, etc.), il est préférable de tenter de les contacter soit par téléphone, soit par mail pour vérifier l'objet de la correspondance et la légitimité de l'envoi.

Enfin, l'étape de sécurité optimale consiste à désactiver l'exécution automatique des macros dans les suites bureautiques de type Microsoft Office (aller dans Fichiers/Options/Centre de gestion de la confidentialité/Paramètre du Centre de gestion de la confidentialité/Paramètres des macros/Désactiver toutes les macros avec notifications).

Comment vérifier sa présence et s'en débarrasser ?

La société française de sécurité Lexsi propose un simple outil de détection permettant tout à la fois de vérifier sa présence sur un ordinateur puis de l'éradiquer complètement. Il est également possible, comme l'explique Lexsi, de nettoyer manuellement son ordinateur.

Téléchargez l'outil sur :
https://www.lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/

Source : http://www.lemonde.fr/pixels/article/2015/10/29/e-mails-pieges-nouvelle-alerte-au-virus-dridex-en-france_4799355_4408996.html

Le Crowdfunding, risques, pièges et précautions à prendre | Denis JACOPINI

Le Crowdfunding, désigne le financement participatif.Est-il risqué ?Quels sont ses pièges ?Quelles sont les précautions à prendre ?

Les petites entreprises aussi victimes de cybercriminalité | Denis JACOPINI

Vols de données clients, piratage de propriété intellectuelle… les cyberattaques sont légion, mais les petites entreprises se croient souvent peu concernées. A tort. Pour se protéger de ces actes malveillants, une bonne « hygiène numérique » simple à mettre en place s'avère nécessaire.

« Dirigeant d'une petite entreprise, vous pensez n'avoir jamais été victime d'une cyberattaque ? Soit vous ne l'avez pas détectée, soit vous n'intéressez plus personne et il faudrait penser à changer de métier ! « .
Cette boutade, destinée à faire prendre conscience aux patrons de PME des risques qu'ils encourent face aux hackers en tout genre, émane du contre-amiral Dominique Riban, directeur général adjoint de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information.
Il faut dire que pour une PME, détecter ne serait-ce que les incidents de sécurité, autrement dit le fait qu'un pirate essaie de s'introduire dans le système sans y parvenir, s'avère bien compliqué. Idem pour les attaques. Certes, des comportements bizarres de l'ordinateur peuvent attirer l'attention, comme son ralentissement, des connexions qui s'effectuent toutes seules, la flèche de la souris qui se ballade… Mais les » méchants » savent surtout se faire discrets. Et il s'agit d'un sujet très – trop – technique, lorsqu'on ne possède pas un collaborateur spécialisé à plein temps pour s'en préoccuper…

Peu de PME portent plainte
Difficile d'avoir des chiffres fiables sur la réalité de la cybercriminalité subie par les PME. Pour une raison simple: peu portent plainte, lorsqu'elles en sont victimes. Pourquoi risquer la mauvaise publicité ? Retrouver l'auteur de l'infraction s'avère de toute façon souvent mission impossible, admet Jean-Louis Di Giovanni, associé PwC du département Litiges et Investigations auteur d'une enquête sur les fraudes en entreprises* : » On peut remonter sa trace, mais quand l'adresse IP provient d'un cybercafé aux alentours de la gare de l'Est, comment voulez-vous mettre la main dessus ? « . Devenir cybercriminel est en tout cas à la portée de tous. » Aujourd'hui, pour une centaine d'euros, vous disposez d'une solution pour attaquer le système d'information de votre concurrent, ou, pour trois fois moins cher, son smartphone « , indique Dominique Riban.

Une menace à plusieurs visages
Fomentée par de malveillants collaborateurs, actuels ou anciens, ou bien perpétrée par des hackers externes, la cybercriminalité s'avère multi-formes. Les attaques ciblées, qui visent à voler un savoir-faire particulier ou des données sensibles (secrets de fabrication, brevets, plans industriels, fichiers clients…), côtoient des attaques que Philippe Humeau, directeur général de NBS System, spécialisée dans l'hébergement de haute sécurité et les tests d'intrusion, nomme d' » opportunistes » : » Il suffit que l'entreprise ait un bout de son système connecté sur le net, qu'elle laisse traîner un mot de passe par défaut, et ça y est, elle est vulnérable. Il faut savoir qu'une adresse IP est scannée vingt fois par jour, explique-t-il. Une vraie industrie, que ces scanners qui recherchent des données relatives à des cartes bleues ou à des » identités « , autrement dit à des informations sur les personnes (celles que l'entreprise doit signaler détenir à la Cnil, ndlr). Aux commandes, des pirates qui effectuent de la récupération massive de données de ce type, puis les revendent au détail à d'autres pirates. » Car elles ont de la valeur. Des données bancaires se revendent dix dollars. Une « identité », entre 5 et 15 dollars. » Une filière aussi organisée que le recel de bijoux « , confirme Dominique Riban.

Des piégeurs pros
Parfois, les cybercriminels entrent carrément en contact avec l'entreprise. Leur inventivité sans faille leur permet de s'engouffrer dans toute nouvelle brèche. Dernier coup à la mode, la » fraude Sepa « . Les entreprises ont, rappelons-le, jusqu'au 31 juillet 2014 maximum, pour opérer leur migration afin d'être conforme à ces nouvelles normes de paiement européennes. Une aubaine, pour les fraudeurs.

Jean-Louis Di Giovanni détaille le processus : » Quelques jours auparavant, ils envoient un mail à la société, pour l'avertir qu'ils vont la contacter par téléphone afin de procéder à des essais. Le mail semble officiel évidemment. On y trouve le numéro du fraudeur, et, comble du raffinement, si l'on appelle, on tombera sur la petite musique d'attente officielle de la banque. Le jour J, ils téléphonent donc à l'entreprise, et demandent à leur interlocuteur de télécharger un programme… qui sert en réalité à prendre la main sur son ordinateur. Le fraudeur voit sur l'écran toutes les informations qu'aurait normalement la banque, et cela le rend ainsi crédible pour passer un ordre, du type : allez sur le compte x sur lequel vous disposez de 2,5 millions d'euros et faites un virement vers ce numéro de compte étranger. » Nombreuses ont été les entreprises à s'exécuter. 48 h plus tard – le délai maximum pour faire bloquer in extremis le virement – c'est trop tard !

80 % de risques évités avec des mesures simples
Des mesures de protection sont aujourd'hui nécessaires. Contrairement aux idées reçues, le recours à des solutions » technologiques » ne constituerait pas forcément la meilleure arme de défense contre les hackers. » Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques « , assure Philippe Trouchaud, associé PwC, spécialiste de la cybersécurité.

L'Anssi publie sur son site un mode d'emploi pour éviter les incidents. Il s'agit d'une quarantaine de » règles d'hygiène « , concernant la sécurité des messageries, du poste de travail, des imprimantes etc. Une quinzaine sont applicables par les petites entreprises. » 80 % des attaques n'auraient pas lieu si ces recommandations étaient respectées « , assure Dominique Riban. Parmi elles, des gestes simples… mais trop souvent négligés. Une évidence, par exemple, de toujours utiliser des mots de passe solides? » 70 % d'entre eux sont faibles, se désole Philippe Humeau. Cette négligence généralisée cause énormément de désastres. Sans compter que les gens utilisent les mêmes partout. »

En plus du choix de mot de passe costauds, les experts font trois recommandations essentielles :

1. Des mises à jour régulières
Se doter d'au moins deux anti-virus et les remettre à jour. » Même si un antivirus n'a jamais été la panacée « , concède le contre-amiral Riban. Même nécessité de remise à jour pour tous ses logiciels. » Si les éditeurs font évoluer leurs versions, c'est parce qu'ils ont constaté des failles de sécurité, pointe Philippe Humeau. Mieux vaut éviter de reporter sans cesse le » rebootage » de sa machine quand elle le demande. »

2. Attention au cloud
Toute nouvelle pratique engendre de nouvelles menaces. C'est le cas du cloud. « N'y stockez pas de données cruciales, exhorte Dominique Riban. Privilégiez des opérateurs français dont vous trouverez la liste sur le site de l'Anssi. Je ne dis pas qu'il n'y aura pas d'accident, mais au moins, notre structure a analysé leur façon de travailler, les a audité, leur a fait corriger leurs failles. Ce n'est pas le cas, par exemple, avec Google ou Microsoft. »

3.Haro sur le BYOD
Philippe Humeau n'hésite pas également à pointer du doigt ce qu'il appelle le » problème des jeunes générations » : » Elles débarquent dans l'entreprise avec des notions de sécurité et de vie privée assez light. Elles ont encore moins de réflexes que leurs aînées. Lorsqu'un jeune n'hésite pas à dévoiler sa cuite du week-end sur Facebook, il ne faut pas s'attendre à ce qu'il sache mettre des barrières là où il devrait les mettre. » Souvent associé à la génération Y – mais pas que – , le phénomène BYOD (» bring your own device «) tient du fléau en matière de cybersécurité. La pratique nécessite d'être encadrée.

 » Il devient difficile de l'interdire, mieux vaut donc accompagner l'usage « , préconise Philippe Humeau. Mettre en place par exemple un réseau internet privé et un autre public, pour que les collaborateurs s'y connectent avec leur machine. Dominique Riban se montre, lui, beaucoup plus radical : » Même si l'appareil appartient à l'employé, seul l'employeur doit pouvoir administrer la machine, afin que l'utilisateur, ou ses enfants, ne puisse pas télécharger tout et n'importe quoi le week-end ou désactiver l'anti-virus. » Pas sûr que les collaborateurs acceptent…

Procéder ou pas à un test d'intrusion
Pour évaluer la capacité de résistance de son système informatique, on peut évidemment faire effectuer un test d'intrusion. A une petite entreprise, il en coûtera aux alentours de 7000 euros. Une facture qui peut paraître prohibitive. » Evidemment cela ne s'adresse pas à tout petit entrepreneur , se défend Philippe Humeau, dont la société propose de tels tests. Mais si l'on a des secrets de fabrication, la dépense est justifiée. Nos interventions se déroulent encore malheureusement trop souvent en post-mortem, nous faisons peu de prévention. »

* Selon cette récente étude, la cybercriminalité est la 2ème fraude la plus signalée en France. Son évolution inquiète particulièrement les dirigeants qui la classent comme la fraude la plus redoutée dans les 24 mois à venir.

Source : http://lentreprise.lexpress.fr/high-tech-innovation/cybercriminalite-les-petites-entreprises-ne-sont-pas-a-l-abri_1518760.html

Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB)

Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB) ?

Déjouer les escroqueries au DAB et adopter les bons gestes pour s'en prémunir, par la brigade des fraudes aux moyens de paiement

Denis JACOPINI :
Parce que nous considérons que notre connaissance des risques et le premier rempart contre les pirates, nos avons souhaité partager avec vous cette vidéo.
N'hésitez pas à nous contacter pour l'organisation de sessions de formations ou de conférences de sensibilisation aux risques informatiques, pour apprendre à vous protéger des pirates, des arnaques et limiter ainsi votre exposition à ces pièges.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Vidéoprotection / vidéosurveillance : le public doit-il être informé qu'il est filmé ? | Denis JACOPINI

Vidéoprotection / vidéosurveillance : le public doit-il être informé qu'il est filmé ?

Les personnes filmées dans un espace public (rue, administration, gare, centre commercial, banque etc.) doivent en être informées, au moyen de panneaux affichés de façon visible comportant :
• Un pictogramme représentant une caméra
• Le nom ou la qualité et le numéro de téléphone du responsable
Ces panneaux doivent être affichés en permanence dans les lieux concernés et doivent être compréhensibles par tous les publics.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source :
https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=514319E089C032799DD14161D6197C4C?name=Vid%C3%A9oprotection%2Fvid%C3%A9osurveillance+%3A+le+public+doit-il+%C3%AAtre+inform%C3%A9+qu%27il+est+film%C3%A9+%3F&id=409

Attaque informatique TV5 Monde – Denis JACOPINI

interviewé par un journaliste de Canal Plus pour le JT de Direct8 | Denis JACOPINI

	Attaque informatique TV5 Monde - Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8

A la suite de l'attaque informatique ayant visé TV5 Monte, le 9 avril dernier, pendant qu'il se trouvait à un Colloque international sur la Cybercriminalité à Montpellier organisé par Adel JOMNI, Denis JACOPINI a été interviewé par un journaliste de Canal Plus et certains propos retenus pour le JT de 20h45 sur Direct 8.

D'après-vous, pourquoi les pirates ont choisi la chaîne de télévision TV5 Monde comme cible de leur attaque informatique ?Lorsque des pirates ou des cybercriminels décident d'attaquer un système informatique, il le font principalement pour les raisons suivantes :- A la suite d'une sorte de défi qu'ils se sont lancés afin de prouver leur capacité à pirater un système qui s'est par exemple déclaré comme système inviolable…- Afin de récolter de l'argent soit en menaçant de diffuser des informations secrètes, soit en vendant les informations piratées, soit en prenant en otage un serveur en le bloquant et tout cela, contre rançon.

– Ou bien, dans le but de diffuser un message idéologique, prônant un message politique, religieux… Dans ce cas, l'objectif premier des cyber-attaquants est la diffusion à grande échelle d'un message (c.f. les deffaçages de plus de 25000 sites Internet à la suite des attentats contre Charlie Hebdo). Que le plus de personnes possibles puisse prendre connaissance d'un message en y associant une sensation de puissance, tel a été le type d'attaque contre TV5 Monde. Cette attaque, a été destinée avant tout à diffuser un message idéologique, en touchant un média à couverture mondiale pour qu'on parle le plus possible des attaquant et de leur symbole.

Quelle a été la technique utilisée lors de l'attaque des serveurs de TV5 Monde ?

Les cybercriminels utilisent généralement 2 types de méthodes pour pénétrer dans un système informatique :

– la recherche de failles

– la naïveté d'un destinataire à un e-mail

C'est un voire même plusieurs e-mails, de type phishing qui semblent être à l'origine, depuis probablement plusieurs semaines ou mois, de l'intrusion du système informatique de TV5 monde par les cybercriminels. Une fois introduits dans le système informatique, l'accès invisible ou silencieux à des informations confidentielles ou secrètes permet ensuite de trouver les clefs autorisant de se répandre dans un réseau et contaminer ainsi le plus possibles d'organes sensibles ou stratégiques.

Une fois tous ces accès ainsi possibles, il suffit de coordonner une attaque simultanée de tous ces fruits devenus véreux pour donner l'impressionnante vision d'un arbre prêt à tomber.

« Il suffit d'envoyer tous les jours un email avec un virus auprès de différentes personnes de différents services et à un moment ou un autre il va bien y a voir quelqu'un qui va l'ouvrir.

Son vrai travail va commencer lorsque quelqu'un aura mordu à l'hameçon »

Peut-on conclure que n'importe quelle chaines de télévision peuvent être victime de cyber-attaques telles que celle dont a été victime TV5 monde ?

La faille qu'ont exploité les cybercriminels dans le cadre de l'attaque informatique de TV5 monde est une faille humaine. En effet, recevoir un e-mail nous incitant à cliquer sur un lien qui va contre notre volonté et de manière complètement invisible changer dans son ordinateur un logiciel malveillant chargé, de manière tout aussi silencieuse, de prendre le contrôle de notre ordinateur est devenu le moyen d'attaque le plus utilisé.

Les systèmes informatiques des chaines de télévision sont certes équipées de moyens de protection techniques contre les virus, les codes malveillants et autres types d'attaques, mais les cybercriminels auront toujours un coup d'avance en exploitant la faille humaine, principalement par manque de connaissance ou manque de formation de la part des utilisateurs.

Existe t-il un moyen de se protéger contre ce type d'attaque ?

Les organismes et entreprises ont prix trop de retard pour mettre en place des politiques de sécurité informatique. Quand on voit qu'en 2013, moins de 100 000 entreprises en France s'étaient mises en conformité avec la CNIL, excellent point de départ pour mettre en place des mesures de sécurité sur les données personnelles, il y a de quoi s'inquiéter sur la manière dont nos données (mot de passe y compris) sont sécurisées.

Commencer par se mettre en conformité avec la CNIL serait un bon début…

http://www.lenetexpert.fr/wp-content/uploads/2015/04/Denis-JACOPINI-interviewé-par-journaliste-Canal-plus-pour-JT-de-Direct-8.mp4

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.bfmtv.com/culture/l-attaque-contre-tv5monde-enclenchee-des-fin-janvier-877334.html

Comment gérer les licences des logiciels installés par les salariés ? | Denis JACOPINI

Comment gérer les licences des logiciels installés par les salariés ?

Dès que l'on souhaite accueillir les terminaux personnels des collaborateurs dans l'entreprise, il faut absolument se pencher sur la question des licences logicielles pour éviter de cuisantes déconvenues.

Dès qu'un logiciel est présent, les risques liés aux licences sont forcément tapis dans l'ombre. Si l'on souhaite accueillir les terminaux personnels des collaborateurs avec un projet BYOD (Bring Your Own Device), il faut donc se pencher sur la question pour éviter de cuisantes déconvenues. Il en va de même avec les petits logiciels gratuits que les employés peuvent installer sur les équipements fournis par l'entreprise, qu'ils en soient ou non administrateurs.

Ces deux exemples, aussi concrets que courants, offrent quelques clefs pour mieux maîtriser un phénomène dont la complexité et l'ampleur ne cessent de croître.

Bring your own licence illégale

Si l'on ne parvient pas à endiguer un phénomène, autant en tirer profit. C'est notamment le cas avec ces équipements informatiques personnels que les employés introduisent discrètement dans les systèmes d'information d'entreprise depuis des années. Las de lutter, les DSI cèdent à une nouvelle mode : le BYOD (Bring Your Own Device).

Certains se contentent de canaliser ces terminaux hétéroclites en veillant à la survie des équipes de support et à la sécurité de l'information : pas de support technique, connexion sur les accès Wi-Fi pour visiteur, etc. D'autres vont plus loin, comme dans cette grande organisation du secteur tertiaire dont je tairai le nom :

· Les collaborateurs peuvent utiliser leur matériel préféré à la place de celui fourni par la DSI ;
· Ils doivent alors y installer l'antivirus homologué dont une licence leur est allouée ;
· S'ils restituent le PC de la compagnie pour n'utiliser que le leur, ce dernier est subventionné ;
· En pareil cas, ils sont livrés à eux-mêmes en termes d'assistance et de logiciels ;
· Ils peuvent cependant bénéficier de l'accord passé avec Microsoft pour acquérir une licence Office à 13 €.

Remarquable exemple de modernité et d'ouverture, qui permet au passage de réduire les coûts de matériel, de logiciel et de support. Le tout est savamment enrobé d'une communication du plus bel effet vantant les mérites d'une transformation digitale soucieuse des collaborateurs et de leur bien-être.

Comme d'habitude, le diable est dans les détails, en l'occurrence dans les conditions d'utilisation de la licence Microsoft Office à 13 €. En effet, elle couvre l'usage secondaire du logiciel sur un PC personnel si une licence entreprise est octroyée à l'utilisateur. Dans notre cas, l'utilisateur n'a plus de licence entreprise puisqu'il l'a restituée en même temps que son PC.

Voilà comment une organisation peut pousser ses collaborateurs à agir illégalement, sans s'exposer directement puisque les logiciels et les terminaux incriminés ne lui appartiennent pas. Les employés mis en défaut par Microsoft pourront cependant prouver qu'ils ont respecté les préconisations relayées par leur hiérarchie. Il n'est pas certain que cela engendre l'atmosphère voulue : décontractée et propice au travail.

La gratuité peut coûter cher

Une autre situation classique, en apparence anodine, peut faire des remous si l'on n'y prend pas garde : les logiciels gratuits, si pratiques et si sympathiques.

Ainsi, un collègue m'a récemment présenté les bienfaits d'un petit freeware qui le comblait d'aise. Il m'a vivement conseillé de l'installer sur mon PC professionnel. Je l'ai donc téléchargé depuis le site de l'éditeur. Avant de lancer l'installation, j'ai lu les conditions d'utilisation (vous auriez évidemment fait la même chose à ma place). Au milieu de cette prose, j'ai découvert que le produit ne devait pas être utilisé en entreprise. Que l'on travaille sur un terminal personnel ou mis à disposition par la DSI ne change rien puisqu'il s'agit toujours d'un usage « en entreprise ». Utiliser ainsi la version gratuite du logiciel est donc illégal.

Disposer des droits d'administrateur sur son ordinateur n'est pas forcément nécessaire pour installer un tel produit. L'entreprise peut donc se retrouver dans une posture inavouable, même si elle a correctement sécurisé son parc informatique. Pour mettre un peu de piment, ajoutons que ces installations occultes passent inaperçues lors des inventaires logiciels, puisqu'ils sont le plus souvent conçus pour détecter ce qui est connu, et non pour découvrir l'inconnu.

De nos jours, les logiciels communiquent presque tous avec leur éditeur via Internet au moyen de protocoles réseau qui franchissent allègrement les dispositifs de sécurité. Il peut s'agir de rechercher des mises à jour ou de fournir des données vous concernant. C'est légal puisque spécifié dans le contrat de licence accepté *de facto* lors de l'installation, qu'il ait été lu ou non. Il suffit alors d'un nombre significatif de PC communiquant depuis votre réseau d'entreprise pour mettre la puce à l'oreille de l'éditeur. Il a alors tout le loisir de vous retrouver grâce à vos adresses IP publiques et de réclamer le manque à gagner en faisant jouer la clause d'audit inscrite, elle aussi, aux conditions générales d'utilisation. Elle lui offre en effet la possibilité de contrôler votre système d'information pour vérifier que les logiciels utilisés sont dûment payés.

Les petits logiciels gratuits peuvent ainsi coûter fort cher à des DSI qui en ignoraient jusqu'à l'existence car les grands éditeurs ne sont plus les seuls à développer leurs ventes par un nouveau canal : l'audit.

L'effort fait les forts

Ces deux cas d'école montrent que la compréhension des contrats de licences est indispensable pour éviter des complications désagréables. C'est par ailleurs un préalable à la gestion des actifs logiciels (Software Asset Management, SAM). Comment, en effet, maîtriser le droit d'usage contractuel d'un produit dont on ignore le contrat ?

En ces temps de crise, la chasse au manque à gagner est ouverte pour de nombreux éditeurs. Tout changement impliquant l'informatique concerne forcément des composants logiciels. Il convient donc d'être prudent et de prendre en considération leur dimension contractuelle. Bien des projets ont vu leur retour sur investissement réduit à néant, voire inversé, après un audit d'éditeur.

En définitive, qu'il s'agisse d'adopter le BYOD, d'utiliser un freeware ou de transformer le système d'information, le SAM renforce la position du client face aux éditeurs de logiciels car, comme disait Marcel Pagnol : « Comme on est faible quand on est dans son tort ! »… [Lire la suite]

Réagissez à cet article

Source : *BYOD et freewares : quid des licences ? – JDN*

Les TPE et les PME, cibles privilégiées des cybercriminels | Denis JACOPINI

Les TPE et les PME, cibles privilégiées des cybercriminels

Selon le spécialiste de la sécurité Symantec, 71 % des TPE et les PME qui font l'objet d'une cyber-attaque ne s'en remettent pas. Pourtant, la sécurité du système informatique ne fait pas partie des priorités des petites et moyennes entreprises, même si c'est un enjeu majeur pour leur survie.

Face à des systèmes d'information de plus en plus ouverts, un usage généralisé d'internet et des terminaux mobiles connectés, les entreprises doivent mettre en œuvre des politiques de sécurité informatique de plus en plus exigeantes. Pourquoi les cybercriminels s'en prennent d'avantage aux TPE et aux PME ? Explication.

La cybercriminalité n'est pas un fait nouveau. Pourtant depuis quelques années, nous sommes tous devenus ultra-connectés et multi-équipés. Ce constat n'épargne pas les entreprises qui ont vu apparaître de nouveaux outils qui permettent aux salariés de rester connecter en étant plus mobile et plus productif. Ces nouveaux modes de travail, sont aujourd'hui autant de failles de sécurité possibles et donc d'attaques possibles. Cette forme de criminalité ne concerne plus les grandes entreprises qui ont majoritairement mis en place des moyens coûteux pour lutter contre le piratage. La nouvelle cible privilégiée des hackers serait les TPE et les PME qui seraient plus simple à attaquer.

Des cibles plus accessibles

Les enquêtes le confirment : les gérants de TPE et PME ont une vision assez exacte du piratage informatique, mais ils se sentent peu concernés. Selon eux, cette forme moderne de criminalité menace surtout les grandes entreprises. Pourtant, les délits constatés contredisent cette perception. Plus encore, le pourcentage des attaques vers les entreprises de moins de 250 salariés progressent. Selon le rapport Symantec Security Threat, elles seraient passées de 18% à 31% en 4 ans. Or ce sont justement les entreprises de moins de 250 salariés qui doivent protéger leurs données. Le constat est le suivant : 40% de la valeur des entreprises est issue des informations qu'elles détiennent. Ce qui intéresse les cybercriminels : dossiers clients, listes de contacts, renseignements sur le personnel et informations bancaires de l'entreprise, cartes de crédit comprises et propriétés intellectuelles. Elles représentent aussi des passerelles d'accès à leurs partenaires.

Un frein pour travailler avec les grandes entreprises

Loin des considérations financières et ne se sentant pas concernées, les TPE et PME s'estiment à l'abri de ces attaques. En conséquence, leurs infrastructures ne sont pas adaptées. Elles sont alors des cibles idéales permettant d'attaquer leurs différents partenaires qui sont parfois des grandes entreprises ou des administrations. Elles deviennent alors un moyen d'accéder à leurs systèmes d'information. Et cela peut constituer un frein à la compétitivité. Les Grandes Entreprises, ne pouvant contrôler le système d'information de leurs partenaires, exigent alors de leurs sous traitants un matériel informatique similaire afin de contrôler les flux.

Des attaques virales invisibles

Les attaques les plus fréquentes sont de natures virales. A l'insu des utilisateurs, elles visent à installer de petits programmes capables d'identifier les mots de passe (via des enregistreurs de frappe), d'accéder aux services bancaires en ligne de l'entreprise (Chevaux de Troie bancaires), de contrôler à distance les ordinateurs de l'entreprise pour lancer des attaques commandées (réseaux de zombies ou botnet) ou d'espionner les employés pour connaître leurs habitudes, leurs mots de passe ou leurs préférences (Spyware)…

De nouvelles attaques plus structurées

Les techniques de piratages évoluent et le matériel n'est plus l'unique faille. On voit apparaître de nouveaux types d'attaques basées sur les failles humaines et sociales. Les environnements de travail des salariés sont ciblés à travers les postes de travail des salariés. A titre d'exemple, les hackers identifient le lien entre les entreprises et leurs partenaires. Des mails sont envoyés depuis les réseaux sociaux type Linkedin ou Viadéo au nom du partenaire. L'email sera donc ouvert sans réel méfiance de la part du salarié. Cette technique, appelée « social engineering », permet alors au pirate d'accéder au poste de travail de l'utilisateur en premier lieu pour ensuite évoluer dans le système d'information de l'entreprise.

Des règles simples de cyber-stratégie

Il n'est pas rare qu'en entreprise les salariés utilisent des outils réservés aux particuliers. Ce type de pratique multiplie les dangers d'intrusion car les systèmes peuvent être piratés. Ils pointeraient vers l'installation de « maliciels » (logiciels malveillants conçus pour infiltrer un ordinateur et y réaliser des activités non autorisées). Il en est de même pour tous les outils connectés. Malheureusement, ce n'est souvent qu'une question de temps avant qu'un hacker arrive à ses fins. Il est donc primordial de faire preuve de plus de rigueur pour gagner du temps afin de décourager l'intrusion. Une entreprise qui connait les risques et montre qu'elle a pris des mesures de sécurité simples, décourage les pirates. Il existe aujourd'hui des services de sécurité informatiques adaptés aux TPE/PME. A titre d'exemple, des prestataires proposent des offres sous forme de machine virtuelle, un proxy complet et simple. Le service permet de filtrer les pages internet en se basant sur des listes préétablies.

Mais bien avant de se consacrer à la sécurisation du matériel de travail, la première mesure à prendre concernera celle des bonnes pratiques des salariés. Des mesures de protection humaines sont nécessaires. « Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques », assure Philippe Trouchaud, associé PricewaterhouseCoopers, spécialiste de la cyber sécurité. Le gouvernement met à disposition un Guide d'Hygiène et de Sécurité de l'ANSSI, il fournit les bases de la sécurité pour les utilisateurs au sein des entreprises.

Aussi une politique de sécurité consistera tout d'abord à mener de front trois actions :
• Identifier les points de vulnérabilité généralement utilisés par les criminels informatiques pour s'introduire dans les systèmes d'information,
• Définir les règles de prudence à appliquer au quotidien par l'entreprise et son personnel,
• Mettre en œuvre systèmes de protection électroniques adéquats. Le tout devant être organisé et planifié dans la durée.

Comment recevoir moins d’appels téléphoniques publicitaires ? | Denis JACOPINI

Comment recevoir moins d’appels téléphoniques publicitaires ?

Règle n° 1 : ne communiquez pas votre numéro de téléphone lors d'un achat ou d'un contact commercial sauf si c'est indispensable (par exemple, pour la livraison).Règle n° 2 : signaler au commerçant que vous ne souhaitez pas que votre numéro soit réutilisé à des fins publicitaires.

Il existe également des listes d'opposition sur lesquelles vous pouvez vous inscrire gratuitement :

• La liste rouge :

Vos coordonnées ne sont pas publiées dans l'annuaire et ne sont pas communiquées par les services de renseignement téléphonique. Contactez votre opérateur télécom.

• La liste orange ou « anti prospection » :

Vos coordonnées sont publiées dans l'annuaire et sont communiquées par les services de renseignement téléphonique. En revanche, elles ne peuvent pas être utilisées pour du démarchage publicitaire. Contactez votre opérateur télécom.

• Liste anti annuaire inversé :

Elle empêche que l'on puisse trouver votre nom ou votre adresse à partir de votre numéro de téléphone fixe ou mobile. Contactez votre opérateur télécom.

A savoir : Votre opérateur telecom peut vous adresser des appels commerciaux sur ses produits et services, même si vous êtes inscrits sur liste rouge ou anti prospection. Pour vous y opposer, contactez votre opérateur.

La liste PACITEL

Vous ne serez plus démarché par les sociétés adhérantes à l'association Pacitel.

MISE A JOUR DU 13/10/2016 :

La liste PACITEL n'existe plus depuis le 1er janvier 2016, elle a été remplacée par BLOCTEL en juin 2016.

Consultez nos infos sur Bloctel : https://www.lenetexpert.fr/bloctel-la-nouvelle-liste-rouge-contre-les-spams-telephoniques

Autre lien : https://www.service-public.fr/particuliers/actualites/A10590

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.aide.cnil.fr/selfcnil/site/template.do?id=112&back=true

Que faire en cas de fraude sur sa carte bancaire ?

Que faire en cas de fraude sur sa carte bancaire ?

De plus en plus d'usagers de la banque sont victimes de l'utilisation frauduleuse de leur carte alors même qu'ils ne l'utilisent pas pour leur achat sur le net. Pourtant il arrive de plus en plus fréquemment que certains d'entre eux constatent des sommes prélevées sur leur compte bancaire en consultant leur relevé bancaire.

Que faire en cas de fraude sur sa carte ? Quelles sont les démarches pour déclarer une utilisation frauduleuse de sa carte bancaire ?

Selon les disposition de l'article L 133-24 du Code Monétaire et Financier, la responsabilité du propriétaire d'une carte bancaire n'est pas engagée dans le cas où la carte a été contrefaite ou si l'achat contesté n'a pas été effectué avec l'utilisation physique de la carte.

Les titulaires de carte victimes d'une utilisation frauduleuse sur Internet ont un délai de 13 mois pour contester les sommes prélevées sur leur compte bancaire. Ils doivent se rendre auprès de sa banque et s'opposer formellement aux transactions effectuées ou au paiement des opérations en question.

Quelles sont les démarches à faire auprès de sa banque ?

En cas d'usurpation des données de sa carte bancaire, il faut :

• Appeler sa banque le plus rapidement possible pour le signaler par téléphone.

• Envoyer à sa banque une lettre qui confirme la mise en opposition de la carte utilisée frauduleusement,

– Un document qui décrit toutes les opérations contestées, les coordonnées bancaires et le motif de l'opposition de la carte,

– Une attestation (AFFIDAVIT) certifiant que la carte a toujours été en sa possession et qu'elle n'a jamais été cédée ou prêtée.

La loi de 2001 sur la protection du consommateur n'exige pas de dépôt de plainte auprès de la gendarmerie. Il n'est donc pas nécessaire de porter plainte pour que la banque procède aux remboursement des sommes usurpées.

Selon les articles L133-19 et L 133-20, la banque doit rembourser toutes les sommes prélevées à compter de la date d'opposition ainsi que tous les frais liés à l'opposition de la carte bancaire.

Pour éviter une usurpation de sa CB, voici quelques conseils et certaines mesures de sécurité à prendre :

– ne jamais laisser la carte bancaire à la vue d'un quelconque public (ex :
– exposée la CB dans la voiture ou sur un bureau),

– penser à reprendre sa carte bancaire dans les terminaux de paiement après chaque achat,

– détruire les tickets de paiement avant de les jeter car ils comportent le code de la carte bancaire,

– ne jamais dire le numéro ni le code secret de la carte bancaire à quiconque,

– ne pas oublier de signer au dos de la carte bancaire.

Source : Banque-en-ligne.fr *Que faire en cas de fraude sur sa carte bancaire ?*
