Victime du ransomware Petya ? Décryptez gratuitement les fichiers | Denis JACOPINI

Victime du ransomware Petya ? Décryptez gratuitement les fichiers

Il est possible de récupérer gratuitement ses fichiers après une infection par le ransomware Petya. Pas forcément simple à mettre en œuvre, une méthode a vu le jour.

Petya bloque totalement l'ordinateur. Pour cela, il écrase le Master Boot Record du disque dur et chiffre la Master File Table sur les partitions NTFS (système de fichiers de Windows). Cette MFT contient les informations sur tous les fichiers et leur répartition.
La procédure malveillante laisse croire à une vérification du disque dur après un plantage et un redémarrage. La victime aura au final droit à une tête de mort en caractères ASCII et une demande de rançon (0,9 bitcoin) pour espérer récupérer ses fichiers et déchiffrer le disque dur prétendument chiffré avec un algorithme dit de niveau militaire.
Un bon samaritain (@leostone) a mis en ligne un outil pour se dépêtrer de Petya (https://petya-pay-no-ransom-mirror1.herokuapp.com) sans devoir payer une rançon. La procédure nécessite de récupérer des données d'un disque dur affecté pour obtenir une clé de déchiffrement promise en quelques secondes. Manifestement, il était simplement question d'un encodage en Base64.
Pour BleepingComputer.com, l'expert en sécurité informatique Lawrence Abrams a confirmé la validité de l'outil. Chercheur en sécurité chez Emisoft, Fabian Wosar a de son côté développé un outil Petya Sector Extractor (http://download.bleepingcomputer.com/fabian-wosar/PetyaExtractor.zip) permettant d'extraire facilement les données à fournir à l'outil de Leostone.
Bien évidemment, le disque dur infecté doit être connecté à un autre ordinateur afin de pouvoir y accéder (extraire les données pour l'outil de Leostone). Une fois la clé de déchiffrement obtenue, il est à replacer dans l'ordinateur d'origine et il faudra saisir la clé sur l'écran affiché par Petya.
L'existence de cette faille pour se débarrasser de Petya sans payer de rançon sera nécessairement portée à la connaissance de l'auteur du ransomware. Le code du nuisible pourrait dès lors être prochainement modifié en fonction.

Source : *Petya : une échappatoire contre le ransomware agressif*

Cyber-Sécurité : des menaces de plus en plus présentes, mais des collaborateurs pas assez formés | Le Net Expert Informatique

	La Cyber-Sécurité de plus en plus menacante, mais des collaborateurs pas assez formés

Les entreprises ont encore trop souvent tendance à sous-estimer le #risque lié au manque de formation de leurs équipes (hors services informatiques) à la cybersécurité. La preuve…

Une enquête réalisée par Intel Security montre que si les collaborateurs de la DSI restent les plus #exposés aux cyberattaques (26 % au niveau européen contre 33 % en France, ce taux étant le plus élevé), les équipes commerciales et les managers (top et middle management) le sont aujourd'hui de plus en plus. En France, 18 % des commerciaux, 17 % du middle management et 14 % des dirigeants sont des #cibles potentielles. Viennent ensuite les personnels d'accueil (5 % en France, taux identique à la moyenne européenne), et le service client (seulement 7 % en France, contre 15 % au niveau européen).
Or ces types de personnel restent tous #mal formés à la sécurité informatique. Le risque est particulièrement fort au niveau des équipes commerciales avec 78 % de professionnels non formés et 75 % des personnels d'accueil. Ces taux descendent un peu pour le top management (65 % de non formés) et pour les équipes du service client (68 %). Côté middle management, la moitié est formée (51 % en France, 46 % au niveau européen).
L'enquête souligne également qu'au-delà des attaques ciblant les personnes non averties via leurs navigateurs avec des liens corrompus, les #attaques de réseaux, les #attaques furtives, les #techniques évasives et les #attaques SSL constituent une menace croissante pour les entreprises. On en recense plus de 83 millions par trimestre. Pour les contrer, les professionnels informatiques français réévaluent la stratégie de sécurité en moyenne tous les huit mois, en ligne avec les pratiques des autres pays européens sondés. 21 % mettent par ailleurs à jour leur système de sécurité moins d'une fois par an (contre 30 % en moyenne au niveau européen). Et 72 % d'entre eux (et 74 % en moyenne en Europe) sont persuadés que leur système de sécurité pourra contrer ces nouvelles générations de cyberattaques.
Or, ils se trompent. Les #attaques DDoS par exemple. Conçues pour créer une panne de réseau et permettre aux hackers de détourner l'attention de l'entreprise, tandis qu'ils se faufilent dans son système et volent des données, elles ne sont pas vraiment prises au sérieux (malgré leur augmentation +165% et leur dangerosité), puisque seuls 20 % des professionnels informatiques français estiment qu'elles constituent la principale menace pour le réseau de leur entreprise.
Au final, il existe un profond décalage entre l'évolution des attaques et la perception qu'en ont les entreprises qui ne peuvent plus négliger la formation de leurs équipes non IT.

Source : http://www.itchannel.info/index.php/articles/157059/cyber-securite-menaces-plus-plus-presentes-mais-collaborateurs-pas-formes.html

---

Anti-phishing, Anti-Malware et protection des

transactions bancaires pour ce logiciel de sécurité | Denis JACOPINI

#Anti-phishing, #Anti-Malware et protection des transactions bancaires pour ce logiciel de sécurité

Maintes fois récompensées par les critiques et les bêta-testeurs, les Editions 2016 des solutions de sécurité ESET sont enfin disponibles. Au programme, de nouvelles interfaces entièrement repensées et un nouvel outil pour sécuriser les transactions bancaires sur ESET Smart Security 9.

En plus des technologies indispensables comme l'**anti-phishing** (pour **se protéger des e-mails de phishing**) et l'**anti-malware** (pour **se protéger des malwares cachés dans des e-mails ou des sites internet infectés**) qui protègent les clients contre les menaces d'Internet, ESET Smart Security 9 contient une toute nouvelle protection des transactions bancaires. Cette fonction met à disposition l'ouverture d'un navigateur sécurisé pour veiller à ce que toutes les transactions financières en ligne soient effectuées en toute sécurité. L'utilisateur peut également paramétrer lui-même tous les sites bancaires de paiement en ligne qu'il consulte le plus fréquemment.

Source :
http://www.tuitec.com/face-a-la-hausse-des-cyberattaques-en-tunisie-eset-lance-ses-nouvelles-solutions/

GDPR compliance: Request for costing estimate

You seem to express an interest in the GDPR (perhaps a little by obligation) and you want to tell us about a project. We thank you for your confidence.
Intervening on Data Protection missions since 2012, after having identified different types of expectations, we have adapted our offers so that they best meet your needs.
Thus, we can assist you in bringing your structure into compliance in several ways : :

1. Are you looking for autonomy ?

We can assist you to learn the essentials of European regulations relating to the Protection of Personal Data and the necessary to understand and start a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized training, or in the form of personalized support;

At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.

2. Do you want to be accompanied for the implementation of compliance ?

We carry out for you the audit which will highlight the points to be improved. At the end of this stage you can, if you wish, achieve compliance or let us proceed with the improvements that you have validated;

At the end of this audit, we will give you a report proving the implementation of corrections as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).

3. Do you want to entrust all of your compliance?

In a perfectly complementary way with your IT service provider and possibly with your legal department, we can take care of the entire process of bringing your establishment into compliance with the GDPR (General Data Protection Regulation) and the various regulations relating to the protection of Personal Data.

From the audit to the follow-up, you can count on our technical and educational expertise so that your establishment is supported externally.

In order to send you a personalized proposal adapted both to the needs of your structure, in accordance with your strategy and your priorities, we would like you to answer these few questions :

We guarantee extreme confidentiality on the information communicated. Persons authorized to consult this information are subject to professional secrecy.

Do not hesitate to communicate as many details as possible, this will allow us to better understand your expectations.

Your First Name / NAME (required)

Your Organization / Company (required)

Your email address (required)

A telephone number (will not be used for commercial prospecting)

You can write us a message directly in the free text area. However, if you want us to establish precise costing for you, we will need the information below.

In order to better understand your request and establish a quote, please provide us with the information requested below and click on the "Send entered informations" button at the bottom of this page for us to receive it. You will receive an answer quickly.

YOUR ACTIVITY

Details about your activity :

Are you subject to professional secrecy? ○Yes◉No○I don't know

Does your activity depend on regulations? ○Yes◉No○I don't know

If "Yes", which one or which ones?

YOUR COMPUTER SYSTEM

Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s) .

Examples :

- 1 WEB server with website to publicize my activity;
- 1 desktop computer with billing software to bill my clients;
- 2 laptops including:

> 1 with email software to correspond with clients and prospects + word processing for correspondence + billing software to bill my clients ...

> 1 with email software to correspond with customers and prospects + accounting software to do the accounting for my company ;

- 1 smartphone with email software to correspond with customers and prospects.

Do you have one or more websites? ○Yes◉No○I don't know

What is (are) this (thoses) website (s)?

Do you have data in the Cloud? ○Yes◉No○I don't know

Which cloud providers do you use?

YOUR PERSONAL DATA PROCESSING

If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)?

SIZING YOUR BUSINESS

Number of employees in your structure : 0

How many of these employees use computer equipment ? 0

Number of departments or departments ** in your structure (example: Commercial service, technical service ...) : 0

Please list the services or departments ** of your structure:

SERVICE PROVIDERS & SUBCONTRACTORS

Do you work with sub-contractors? ○Yes◉No○I don't know

Please list these subcontractors :

Do you work with service providers who work on your premises or in your agencies (even remotely) ? ○Yes◉No○I don't know

Please list these providers :

How many IT companies do you work with ? 0

Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment :

YOUR SITUATION TOWARDS THE GDPR

Does your establishment exchange data with foreign countries ? ○Yes◉No○I don't know

If "Yes", with which country(ies)?

Have you already been made aware of the GDPR ? ○Yes◉No○I don't know

Have people using IT equipment already been made aware of the GDPR ? ○Yes◉No○I don't know

If you or your employees have not been made aware of the GDPR, would you like to undergo training ? ○Yes◉No○I don't know

YOUR WORKPLACE

The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process.

Do you have several offices, agencies etc. legally dependent on your establishment ? ○Yes◉No

If "Yes", how much ? 0

In which city (ies) (and country if not in France) do you or your employees work ?

TYPE OF SUPPORT DESIRED

We can support you in different ways.

A) We can teach you to become autonomous (training) ;

B) We can support you at the start and then help you become independent (support, audit + training) ;

C) We can choose to entrust us with the entire process of compliance (support) ;

D) We can accompany you in a personalized way (thank you to detail your expectations).

What type of support do you want from us (A / B / C / D + details) ?

END OF QUESTIONNAIRE

If you wish, you can send us additional information such as:

- Emergency of your project;
- Any additional information that you deem useful to allow us to better understand your project.

Send entered informations

[block id="24086" title="Mentions légales formulaires"]

** = for example, commercial service, technical service, educational service, administrative and financial service ...

A

or send an email to rgpd[at]lenetexpert.fr

Denis JACOPINI is our Expert who will accompany you in your compliance with the GDPR.

Let me introduce myself: Denis JACOPINI. I am an expert in sworn IT and specialized in GDPR (protection of Personal Data) and in cybercrime. Consultant since 1996 and trainer since 1998, I have experience since 2012 in compliance with the regulations relating to the Protection of Personal Data. First technical training, CNIL Correspondent (CIL: Data Protection Correspondent) then recently Data Protection Officer (DPO n ° 15845), as a compliance practitioner and trainer, I support you in all your procedures for compliance with the GDPR.

« My goal is to provide all my experience to bring your establishment into compliance with the GDPR. »

La Méthode EBIOS désormais adaptée aux traitements de données à caractère personnel et à la CNIL | Denis JACOPINI

	La Méthode EBIOS, élaborée par l'ANSSI, initialement prévue pour la gestion des risques informatiques a été adaptée aux traitements de données personnelles Parmi les méthodes d'identification des risques en sécurité Informatique, la méthode EBIOS a été retenue par la CNIL en raison de sa simplicité de mise en oeuvre.

1. Objectifs

Dans une entreprise, les risques liée à l'utilisation de l'outils informatique peuvent être classés en deux principales catégories :

– Les risques liés au fonctionnement de l'outil informatique et à la sécurité d'accès au système;

- les risques liés à l'usage des données présentes dans le système informatique.

La gestion du premier risque est en général déléguée au responsable informatique ou, pour des structures de taille plus importantes, au Directeur ou Responsable des services d'information (DSI) et, pour des structures de tailles encore plus importantes, confiée au Responsable de la Sécurité des Services d'Information.
Dans la longue liste des recommandations liées à la gestion de

ces risques nous trouvons la gestion du fonctionnement du système informatique, la sécurité des données (garantie de pérennité et protection contre la fuite de de données) mais aussi la sécurité du système informatique contre les erreurs de manipulations et actes malveillants.

Par contre, la gestion des risques liés à l'usages des données, et plus particulièrement des données personnelles, est répartie entre l'utilisateur, le responsable des traitements (souvent le chef d'entreprise dans des structures de petite taille) et le correspondant Informatique et libertés.

Si l'utilisateur doit bien veiller à une utilisation responsable en évitant par exemple de quitter son poste sans verrouiller l'ordinateur

---

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

---

2. Introduction à la méthode EBIOS

Parmi les méthodes d'identification des risques en sécurité Informatique, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a été retenue par la CNIL en raison de sa simplicité de mise en oeuvre.

La méthode, élaborée et tenue à jour par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), en charge notamment, de la protection de l'état, initialement prévue pour être utilisée dans l'analyse de systèmes informatiques complexes, a été simplifiée et adaptée par la CNIL aux traitements de données personnelles et à la protection de la vie privée qui lui est associée

Cet article décrit les étapes de la démarche à appliquer pour réaliser une étude des risques qu'un traitement de Données à Caractère Personnel fait peser sur la vie privée. Il décrit la manière d'employer la méthode EBIOS dans le contexte spécifique « informatique et libertés ».

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

---

3. Les 5 étapes essentielles

On souhaite éviter les situations suivantes :

- indisponibilité des processus ;

- modification du traitement (détournement de la finalité, collecte excessive ou déloyale…) ;
- accès illégitime aux Données à Caractère Personnel ;
- modification non désirée des Données à Caractère Personnel ;
- disparition des Données à Caractère Personnel ;

La méthode EBIOS consiste, en fonction de l'environnement de départ, à décomposer en 5 étapes (que nous allons étudier en détail) permettant de passer en revue l'ensemble des mesures préconisées dans leur domaine spécifique, en repérer les points de faiblesses c'est-à-dire les vulnérabilités, d'estimer via une étude de risque, les capacités que semblent avoir les sources de risques à exploiter les vulnérabilités pour réaliser une menace, et enfin de mettre en place des mesures techniques et organisationnelles permettant de remédier aux vulnérabilités qu'elle peut présenter.

1. Etude du contexte :
   Quel est le sujet de l'étude ?
   Pourquoi et comment va-t-on gérer les risques ?

2. Étude des événements redoutés :
Quels sont les événements craints ?
Quels seraient les plus graves ?

3. Étude des menaces :
Quels sont les scénarios possibles ?
Quels sont les plus vraisemblables ?

4. Étude des risques :
Quelle est la cartographie des risques ?
Comment choisis-t-on de les traiter ?

5. Étude des mesures de sécurité :
Quelles mesures devrait-on appliquer ?
Les risques résiduels sont-ils acceptables ?

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

---

4. Les 5 étapes en détail

4.1. Etude du contexte : De quoi parle t-on ?

Le but de cette étape est d'obtenir une vision claire du périmètre considéré en identifiant tous les éléments utiles à la gestion des risques, en répondant aux questions suivantes :

4.1.1 Quels sont les éléments à protéger ?

- Quel est le traitement concerné ?
- Quelle est sa finalité (voir les articles 6 et 9 de la loi Informatique et Libertés)?
- Quels sont ses destinataires ?
- Quel est le processus métier que le traitement permet de réaliser ?
- Quelles sont les personnes concernées par le traitement ?
- Comment les processus légaux vont-ils être mis en oeuvre ?
- Quelles sont les DCP du traitement considéré ?
- Quelles sont les DCP utilisées par les processus légaux ?

4.1.2 Quels sont les supports des éléments à protéger ?

- Quels sont les matériels (ordinateurs, routeurs, supports électroniques…) ?
- Quels sont les logiciels (systèmes d'exploitation, messagerie, base de données, applications métier…) ?
- Quels sont les canaux informatiques (câbles, WiFi, fibre optique…) ?
- Quelles sont les personnes impliquées?
- Quels sont les supports papier (impressions, photocopies…) ?

- Quels sont les canaux de transmission papier (envoi postal, circuit de validation…) ?

4.1.3 Quels sont les principaux bénéfices du traitement pour les personnes concernées ou la société en général ?

4.1.4 Quelles sont les principales références à respecter (réglementaires, sectorielles…) ?

4.1.5 Quelles sont les sources de risques pertinentes qui peuvent être à l'origine de risques dans le contexte particulier du traitement considéré ?

- Quelles sont les personnes internes à considérer (utilisateur, administrateur,
- développeur, décideur…) ?
- Quelles sont les personnes externes à considérer (client, destinataire, prestataire,
- concurrent, militant, curieux, individu malveillant, organisation gouvernementale,
- activité humaine environnante…) ?
- Quelles sont les sources non humaines à considérer (sinistre, code malveillant
- d'origine inconnue, phénomène naturel, catastrophe naturelle ou sanitaire…) ?

4.2 Étude des événements redoutés : Que craint-on qu'il arrive ?

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de tous les événements redoutés dans le cadre du traitement considéré et d'en mesurer leur valeur de danger.

Pour expliciter les événements redoutés, leurs impacts potentiels doivent être identifiés :
quelles pourraient être les conséquences sur l'identité des personnes concernées, leur vie privée, les droits de l'homme ou les libertés publiques pour chacun des événements redoutés, c'est-à-dire si :

- les processus légaux n'étaient pas disponibles ?
- le traitement était modifié ?
- une personne non autorisée accédait aux DCP ?
- les DCP étaient modifiées ?
- les DCP disparaissaient ?

Afin de hiérarchiser les événements redoutés, la gravité est déterminée en mesurer la facilité avec laquelle on peut identifier les personnes concernées et l'importance des dommages des impacts potentiels.

Avec quelle facilité peut-on identifier les personnes concernées ? (1 à 4)

- 1. Négligeable : il semble quasiment impossible d'identifier les personnes à l'aide des Données à Caractère Personnel les concernant (ex. : prénom seul à l'échelle de la population française).
- 2. Limité : il semble difficile d'identifier les personnes à l'aide des DCP les concernant, bien que cela soit possible dans certains cas (ex. : nom et prénom à l'échelle de la population française).
- 3. Important : il semble relativement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom et date de naissance, à l'échelle de la population française).
- 4. Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom, date de naissance et adresse postale, à

l’échelle de la population française).

Quelle serait l’importance des dommages correspondant à l’ensemble des impacts potentiels ? (1 à 4)

- 1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu’elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement…).
- 2. Limité : les personnes concernées pourraient connaître des désagréments significatifs, qu’elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d’accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure…).
- 3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu’elles devraient pouvoir surmonter, mais avec de sérieuses difficultés (détournements d’argent, interdiction bancaire, dégradation de biens, perte d’emploi, assignation en justice, aggravation de l’état de santé…).
- 4. Maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu’elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès…).

Mesure de la gravité = Facilité d’identification des personnes + importance des dommages

4.3 Étude des menaces : Comment cela peut-il arriver ?

Cette étape est optionnelle si la gravité précédemment calculée est négligeable (1) ou limitée (2).

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de toutes les menaces qui permettraient aux événements redoutés de survenir.

Vulnérabilités des supports

Risque à anticiper :

- Détérioration d'un matériel (ex. : destruction d'un serveur)
- Usage anormal d'un logiciel (ex. : maladresse en manipulant les fichiers)
- Départ d'une personne (ex. : démission de celui qui connait les procédures)
- Disparition d'un canal papier (ex. : changement de procédures)
- Vol d'un matériel (ex. : vol d'un PC portable dans le train)
- Détournement d'usage d'un logiciel (ex. : usage à titre personnel)
- Modification d'un logiciel (ex. : propagation d'un virus)

Dans quelle mesure les caractéristiques des supports sont-elles exploitables pour réaliser la menace ?

- 1. Négligeable : il ne semble pas possible de réaliser

la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l’organisme dont l’accès est contrôlé par badge et code d’accès).

- 2. Limité : il semble difficile de réaliser la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l’organisme dont l’accès est contrôlé par badge).
- 3. Important : il semble possible de réaliser la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d’un organisme dont l’accès est contrôlé par une personne à l’accueil).
- 4. Maximal : il semble extrêmement facile de réaliser la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l’organisme).

Capacités des sources de risques sont estimées pour chaque menace

Quelles sont leurs capacités à exploiter les vulnérabilités (compétences, temps disponible, ressources financières, proximité du système, motivation, sentiment d’impunité…) ?

- 1. Négligeable : les sources de risques ne semblent pas avoir de capacités particulières pour réaliser la menace (ex. : détournement d’usage de logiciels par une personne sans mauvaises intentions ayant des privilèges restreints).
- 2. Limité : les sources de risques ont quelques capacités, mais jugées peu importantes, pour réaliser la menace (ex. : détournement d’usage de logiciels par une personne mal intentionnée ayant des privilèges restreints).
- 3. Important : les sources de risques ont des capacités

réelles, jugées importantes, pour réaliser la menace (ex. : détournement d’usage de logiciels par une personne sans mauvaises intentions ayant des privilèges d’administration illimités).

- 4. Maximal : les sources de risques ont des capacités certaines, jugées illimitées, pour réaliser la menace (ex. : détournement d’usage de logiciels par une personne mal intentionnée ayant des privilèges d’administration illimités).

Vraisemblance des menaces = Mesure de la vulnérabilités des supports + Capacités des sources de risques

Exemples de menaces qui peuvent affecter la confidentialité

Exemples de menaces qui peuvent affecter l’intégrité

Exemples de menaces qui peuvent affecter la disponibilité

4.4 Étude des risques : quel est le niveau des risques ?

Le but de cette étape est d'obtenir une cartographie des risques permettant de décider de la priorité de traitement.
Puisqu'un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne :

- sa gravité est égale à celle de l'événement redouté,
- sa vraisemblance est égale à la valeur la plus élevée de la vraisemblance des menaces associées à l'événement redouté.

On peut dès lors positionner les risques sur une cartographie :

En fonction du positionnement de vos risques au sein de la cartographie ci-dessus, vous pouvez par ordre de priorité, vous fixer des objectifs :

Zone n°1 : La gravité des risques est élevée, mais la vraisemblance faible
Ces risques doivent être évités ou réduits, par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devront être privilégiées ;

Zone n°2 : La gravité et la vraisemblance sont élevées
Ces risques doivent absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;

Zone n°3 : La gravité et la vraisemblance sont faibles
Ces risques peuvent être pris, d'autant plus que le traitement

des autres risques devrait également contribuer à leur traitement.

Zone n°4 : La gravité est faible mais la vraisemblance élevée
Ces risques doivent être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devront être privilégiées ;

4.5 Étude des mesures de sécurité : Quelles mesures devrait-on appliquer ?

Le but de cette étape est de bâtir un dispositif de protection qui permette de traiter les risques de manière proportionnée, qui soit conforme à la Loi informatique et Libertés, et qui tienne compte des contraintes du responsable de traitement (légales, financières, techniques…).

Tout d'abord, il convient de déterminer les mesures pour traiter les risques. Pour ce faire, il est nécessaire de relier les mesures existantes ou prévues (identifiées précédemment dans l'étude ou dans les références applicables) au(x) risque(s) qu'elles contribuent à traiter.

Des mesures sont ensuite ajoutées tant que le niveau des risques n'est pas jugé acceptable.

Cette action consiste à déterminer des mesures complémentaires qui vont porter :

1. sur les éléments à protéger : mesures destinées à empêcher que leur sécurité ne puisse être atteinte, à détecter leur atteinte ou à recouvrer la sécurité informer les personnes concernées, minimiser les DCP, anonymiser les DCP…) ;
2. puis, si ce n'est pas suffisant, sur les impacts potentiels : mesures destinées à empêcher que les

conséquences du risque ne puissent se déclarer, à identifier et limiter leurs effets ou à les résorber (sauvegarder, contrôler l'intégrité, gérer les violations de DCP…) ;

3. ensuite, si ce n'est pas suffisant, sur les sources de risques : mesures destinées à les empêcher d'agir ou de concrétiser le risque, à identifier et limiter leur action ou à se retourner contre elles (contrôler les accès physiques et logiques, tracer l'activité, gérer les tiers, lutter contre les codes malveillants…) ;
4. enfin, si ce n'est pas suffisant, sur les supports : mesures destinées à empêcher que les vulnérabilités puissent être exploitées, à détecter et limiter les menaces qui surviennent tout de même ou à retourner à l'état de fonctionnement normal (réduire les vulnérabilités des logiciels, des matériels, des personnes, des documents papiers…).

Remarque :

Plus les capacités des sources de risques sont importantes, plus les mesures doivent être robustes pour y résister.
Par ailleurs, les éventuels incidents qui auraient déjà eu lieu, notamment les violations de DCP, ainsi que les difficultés rencontrées pour mettre en oeuvre certaines mesures, peuvent servir à améliorer le dispositif de sécurité.
Les mesures spécifiées devraient être formalisées, mises en place, auditées de manière régulière et améliorées de manière continue.

Il convient ensuite de ré-estimer la gravité et la vraisemblance des risques résiduels (c'est-à dire les risques qui subsistent après application des mesures choisies) en tenant compte de ces mesures complémentaires. Il est alors possible de les repositionner sur la cartographie ci-dessous :

Enfin, il convient d'expliquer pourquoi les risques résiduels peuvent être acceptés.

Cette justification peut s'appuyer sur les nouveaux niveaux de gravité et de vraisemblance et sur les bénéfices du traitement identifiés précédemment (prise de risques au regard des bénéfices attendus) en appliquant les règles suivantes :

Zone n°1 : Risques dont la gravité est élevée mais la vraisemblance faible
Ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable ;

Zone n°2 : Risques dont la gravité et la vraisemblance sont élevées
Ces risques ne doivent pas être pris ;

Zone n°3 : Risques dont la gravité et la vraisemblance sont faibles
Ces risques peuvent être pris.

Zone n°4 : Risques dont la gravité est faible mais la vraisemblance élevée : ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;

Remarque :

Il peut être acceptable de déroger à ces règles, mais uniquement s'il est démontré que les
bénéfices du traitement sont largement supérieurs aux risques.

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

Références :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

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 à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Les petites entreprises aussi

victimes de cybercriminalité | Denis JACOPINI

	Les petites entreprises aussi victimes de cybercriminalité

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.

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

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

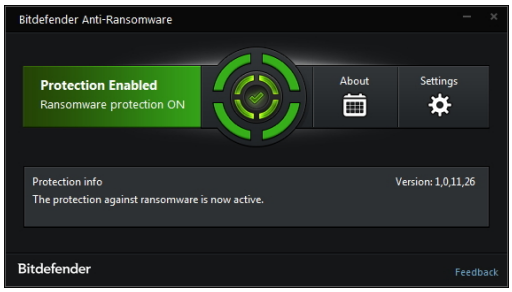
Des règles simples de cyber-stratégie

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.

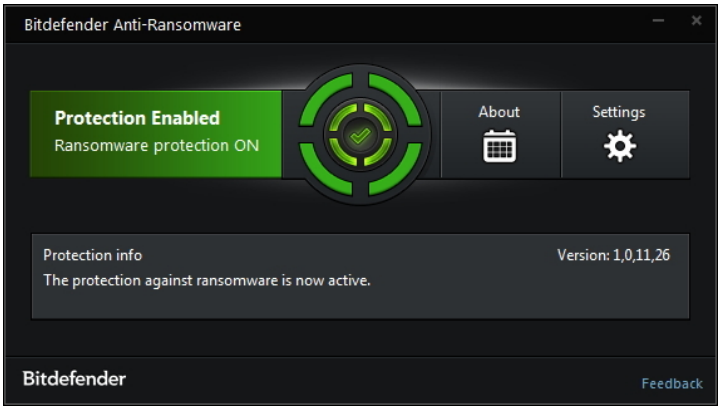
Aussi une politique de sécurité consistera tout d'abord à mener de front trois actions :
• Identifier les points de vulnérabilité généralement utilisés par les criminels informatiques pour s'introduire dans les systèmes d'information,
• Définir les règles de prudence à appliquer au quotidien par l'entreprise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

Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ? | Denis JACOPINI



Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ?

Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.



Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.

The new Bitdefender Anti-Ransomware vaccine is built on the same principle as a previous tool that the company designed to prevent CryptoWall infections. CryptoWall later changed the way in which it operates, rendering that tool ineffective, but the same defense concept still works for other ransomware families.
While security experts generally advise against paying ransomware authors for decryption keys, this is based more on ethical grounds than on a perceived risk that the keys won't be delivered.
In fact, the creators of some of the most successful ransomware programs go to great lengths to deliver on their promise and help paying users decrypt their data, often even engaging in negotiations that result in smaller payments. After all, the likelihood of more users paying is influenced by what past victims report.
Many ransomware creators also build checks into their programs to ensure that infected computers where files have already been encrypted are not infected again. Otherwise, some files could end up with nested encryption by the same ransomware program.
The new Bitdefender tool takes advantage of these ransomware checks by making it appear as if computers are already infected with current variants of Locky, TeslaCrypt or CTB-Locker. This prevents those programs from infecting them again.
The downside is that the tool can only fool certain ransomware families and is not guaranteed to work indefinitely. Therefore, it's best for users to take all the common precautions to prevent infections in the first place and to view the tool only as a last layer of defense that might save them in case everything else fails.
Users should always keep the software on their computer up to date, especially the OS, browser and browser plug-ins like Flash Player, Adobe Reader, Java and Silverlight. They should never enable the execution of macros in documents, unless they've verified their source and know that the documents in question are supposed to contain such code.
Emails, especially those that contain attachments, should be carefully scrutinized, regardless of who appears to have sent them. Performing day-to day activities from a limited user account on the OS, not from an administrative one, and running an up-to-date antivirus program, are also essential steps in preventing malware infections.
« While extremely effective, the anti-ransomware vaccine was designed as a complementary layer of defense for end-users who don't run a security solution or who would like to complement their security solution with an anti-ransomware feature, » said Bogdan Botezatu, a senior e-threat analyst at Bitdefender, via email… [Lire la suite]

Réagissez à cet article

Source : *Free Bitdefender tool prevents Locky, other ransomware infections, for now | Computerworld*

Comment vérifier si votre site Internet a été victime d'un Hackeur | Denis JACOPINI

	Que ça soit à cause d'une simple erreur de frappe ou du fait que votre site Internet a été Hacké, l'auteur, l'éditeur ou le rédacteur en chef d'un site Internet peut être pénalement responsable des conséquences causées par son contenu non désiré.

Afin de vérifier si votre site Internet a été Hacké, voici quelques conseils pour vérifier si votre site Internet a été victime d'un Hackeur :

Que votre site Internet ait été victime d'un hackeur ou que votre site Internet ait été victime d'un pirate sont deux choses différentes.

Le pirate va pomper une partir ou la totalité du contenu de votre site Internet. Le hackeur va modifier le contenu de votre site Internet dans un but de malveillance.

Les conseils que je vais vous donner concernent le cas où un site Internet a été Hacké.

DU CONTENU ETRANGE APPARAIT ?

En premier lieu, consultez votre site Internet sur plusieurs ordinateurs ayant des systèmes d'exploitation et des navigateurs différents afin de vérifier si un affichage anormal apparaît.

UN ANTIVIRUS DECLENCHE UNE ALERTE A L'OUVERTURE DE VOTRE SITE INTERNET ?

Un message d'alerte de votre antivirus est aussi un bon indicateur de la présence éventuelle d'un code suspicieux sur votre site Internet.

Première solution : Depuis votre dernière sauvegarde vous n'avez plus fait de modifications :

Restaurez les pages Web ou la base de donnée contaminée.

Seconde solution : Vous n'avez pas de Sauvegarde de votre site Internet ou la sauvegarde est trop vieille :

Dans ce cas, vous allez devoir résoudre le problème à la main.

COMMENT TESTER VOTRE SITE INTERNET

Enfin, si vous ne savez pas si votre site Internet a été hacké, vous pouvez le vérifier en utilisant les outils suivants :

https://www.virustotal.com/url

VirusTotal est un service gratuit qui *analyse les fichiers et URL suspects*, et facilite la détection rapide des virus, vers,

trojans et tous types de malwares.

http://www.urlvoid.com
URLVoid.com is a free service developed by NoVirusThanks Company Srl that allows users to scan a website address with multiple website reputation engines and domain blacklists to facilitate the detection of possible dangerous websites, used to distribute malware and spyware or related to fraudulent activities.

http://urlquery.net
Query.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

http://wepawet.iseclab.org/
Dans ce cas, vous allez devoir résoudre le problème à la main.

COMMENT SE PROTEGER D'UN HACKEUR ?

Voici quelques astuces simples vous aideront a protéger votre site efficacement contre les pirates et hackers de l'internet :

Ces techniques sont efficace contre les hackers débutants.

- Avoir un hébergeur de qualité et lui même utilisant des surveillances automatiques et permanentes.
- Mettez à jour systématiquement le système d'exploitation de votre serveur ainsi que toutes les applications liées à l'hébergement des sites internet, du FTP, des messageries et des bases de données.
- Supprimer l'utilisateur « admin » des logiciels et créez le votre
- Mot de passe sécurisé (minuscules, majuscules, chiffres et symboles)

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)