Association Nationale des Directeurs
et Directeurs-Adjoints des Centres De Gestion
de la Fonction Publique Territoriale

LES COLLECTIVITÉS TERRITORIALES FACE À LA *cybercriminalité*

EN PARTENARIAT AVEC :

GRAS SAVOYE
Willis Towers Watson

Association Nationale des Directeurs
et Directeurs-Adjoints des Centres De Gestion
de la Fonction Publique Territoriale

LES COLLECTIVITÉS TERRITORIALES FACE À LA *cybercriminalité*

Ce guide a été réalisé par Zineb Lebik, Directrice du département Gestion locale du CIG de la Grande Couronne, Christophe Chassagne, Responsable du service Conseil en informatique et télécommunications du CIG de la Grande Couronne, Stéphane Dahan, Responsable Sécurité Informatique et des Réseaux chez Securiview, Frédéric Gard, Responsable Pôle Santé chez Gras Savoye et Rémy Février, Maître de Conférences au CNAM, Responsable des Unités d'Enseignement « Management et Audit des Systèmes d'Information », ancien Lieutenant-Colonel de la Gendarmerie Nationale.

/ EDITION 2016

EN PARTENARIAT AVEC :

GRAS SAVOYE
Willis Towers Watson

Avant-PROPOS

Les enjeux de la sécurité informatique sont aujourd'hui nombreux et les collectivités territoriales doivent faire face à des menaces liées à l'utilisation des outils informatiques et à la dématérialisation de certaines procédures : intrusions, vols d'informations (état-civil, plateforme marchés publics, fichiers scolaires et périscolaires…). Les conséquences peuvent être lourdes en termes de protection des données et de gestion des services.

Se trouvant démunies de repères dans la gestion des risques informatiques et face à des utilisateurs parfois imprudents, les collectivités investissent dans des protections très couteuses ou bien n'ont pas réellement conscience des répercussions, alors que des solutions simples peuvent être mises en place.

Aussi, l'ANDCDG a souhaité mettre à leur disposition un guide leur permettant d'avoir une approche pragmatique et globale, que le lecteur soit élu ou agent territorial, de tous les risques encourus, des bonnes pratiques à adopter, ainsi que des solutions en terme d'assurance et de protection juridique.

L'ANDCDG tient à remercier les experts en matière de sécurité informatique qui ont contribué à la rédaction de ce guide et pour l'enrichissement qu'ils y ont apporté : Stéphane Dahan, Responsable Sécurité Informatique et des Réseaux chez Securiview, Frédéric Gard, Responsable Pôle Santé chez Gras Savoye et Rémy Février, Maître de Conférences au CNAM, Responsable des Unités d'Enseignement « Management et Audit des Systèmes d'Information », ancien Lieutenant-Colonel de la Gendarmerie Nationale.

Jean-Laurent Nguyen Khac
Président de l'ANDCDG

Sommaire

Introduction

Si chaque jour apporte de nouveaux exemples de cybermenaces pesant désormais sur l'ensemble des organisations publiques ou privées, force est de constater que le traitement médiatique de ces dernières se limite le plus souvent à la mise en exergue d'affaires emblématiques liées à un piratage d'origine étatique (affaire Snowden…) ou d'attaques numériques touchant des entités particulièrement symboliques (TV5 Monde, Ministère des Finances…). Or, ces quelques cas spécifiques ne doivent pas occulter le fait que de nombreuses autres menaces numériques existent et notamment celles visant des collectivités territoriales bien peu conscientes des risques numériques qui pèsent dorénavant sur elles.

Notre thèse de doctorat consacrée au management de la Sécurité des Systèmes d'Information (SSI) des collectivités territoriales françaises a mis en évidence le fait selon lequel la très grande majorité des élus locaux n'a toujours pas pris la mesure des menaces numériques, alors même qu'à la suite des attentats de janvier 2015, plusieurs centaines de sites Web de collectivités territoriales ont fait l'objet d'un défaçage. Le ciblage de ces dernières s'explique à la fois par leur importance au sein de la communauté nationale, ainsi que du fait des défis numériques auxquels elles sont dorénavant confrontées et qui constituent autant d'opportunités pour des cyberpirates cherchant à maximiser l'impact sociétal de leurs attaques.

En effet, parties prenantes des évolutions de la société dans son ensemble et de l'environnement économique, le fait qu'elles soient constituées d'individus issus de toutes les classes d'âges et de tous les milieux, font des collectivités territoriales de parfaites vigies des mutations économiques et sociétales. Les élus locaux étant devenus les dépositaires d'attentes souvent divergentes, voire antagonistes, ils demeurent, plus que jamais, les garants de l'intérêt général, ce qui les contraint à une quasi-obligation de résultat, relativement à un impératif de développement harmonieux du territoire dont ils ont la charge.

Or, depuis une dizaine d'années, ces territoires sont soumis à des mutations sans précédent sous l'influence conjuguée d'évolutions sociétales majeures et de restrictions budgétaires dont l'impact simultané oblige les élus locaux à revoir en profondeur leurs processus de management ainsi que leur approche de l'environnement extérieur.

La recherche d'une nouvelle rationalité territoriale, illustrée par une gestion plus dynamique et prospective des ressources humaines et financières de la collectivité, ne constitue, néanmoins, qu'une étape dans le processus de prise en compte d'une nouvelle réalité. Les nouvelles technologies ont profondément modifié la définition et le champ de la citoyenneté, tout en induisant des changements majeurs dans l'exercice des responsabilités électives. L'appropriation, par les collectivités territoriales, de l'ensemble des opportunités offertes par les Technologies de l'Information et de la Communication (TIC), s'impose donc aujourd'hui comme un impératif absolu, que ce soit en tant que vecteur communicationnel extérieur ou comme axe organisationnel stratégique.

Cependant, la prise en compte des TIC par les collectivités territoriales ne constitue pas uniquement un choix raisonné, fondé sur la volonté de dialoguer avec l'environnement extérieur et les administrés ou d'améliorer leur gestion interne : plusieurs impératifs s'imposent à elles en termes de mise en place et d'utilisation de nouveaux vecteurs de communication. Sous la pression conjointe d'un continuum gouvernemental soucieux d'améliorer la qualité des prestations rendues aux citoyens et de renforcer les liens entre les acteurs économiques locaux et les instances européennes privilégiant les TIC pour améliorer la démocratie participative, les collectivités territoriales sont dorénavant amenées à relever trois défis numériques majeurs face auxquels elles paraissent souvent démunies : l'administration électronique, l'e-démocratie et la dématérialisation des appels d'offres.

Cette utilisation, chaque jour plus étendue des Systèmes d'Information (SI) par les collectivités territoriales, conduit à encourager ces dernières à mieux protéger leur SI au travers de la mise en place minimale de précautions simples et de bon sens, ainsi qu'idéalement, de la réalisation d'un véritable schéma directeur stratégique de Sécurité des Systèmes d'Information au sein de la collectivité. Ces actions de protection apparaissent dorénavant d'autant plus indispensables que la responsabilité du président de l'exécutif local peut potentiellement être engagée sur les plans civil et pénal (vols de données à caractère personnel, utilisation illégale d'un poste de travail par un agent…) en cas d'insuffisance manifeste dans la protection du Système d'Information de sa collectivité.

Ce guide constitue donc une excellente initiative qui vise à mettre à disposition des élus locaux et des fonctionnaires territoriaux en charge de ces problématiques, des fiches didactiques et à visée directement opérationnelle afin de commencer à prendre en main la SSI au sein de leur organisation respective.

Rémy Février

.

Rémy Février est Docteur en sciences de gestion et Maître de conférences au CNAM où il dirige les unités d'enseignement « Management et Audit des Systèmes d'Information ». Ancien officier supérieur de Gendarmerie expert en Intelligence Economique et Sécurité des Systèmes d'Information, il est également Maître de conférences à ESCP Europe et professeur affilié à l'EM Normandie en Intelligence Economique et gestion des risques numériques.

Les principales
MENACES ACTIVES

LES PRINCIPALES MENACES ACTIVES

L'actualité des menaces actives est assez large et surtout non-exhaustive. Chaque jour, une nouvelle menace sur les systèmes d'information vient s'ajouter à celle de la veille. La protection des données est de plus en plus importante à mettre en œuvre. Elle est souvent négligée au prétexte de « coûts importants » mais il s'avère dans tous les cas que les dégâts causés par une attaque (quelle qu'elle soit mais avec pour but de détruire les données), coûte bien plus cher en termes financiers et aussi en termes d'image. Car au-delà de la simple perte de données, qui est maintenant répréhensible si des mesures suffisantes n'ont pas été prises, il y a l'image de la collectivité qui peut être entachée dans ce type d'attaque.

Les attaques les plus en vogue dans ces derniers mois sont des attaques en fishing (tentative d'extorquer des codes via un mail piégé) et surtout des attaques via ransomware. Ces dernières consistent à envoyer, dans une pièce jointe de type bureautique, un code malveillant qui va chiffrer toutes les données informatiques sur lesquelles vous avez un droit d'accès. Ce chiffrement est irréversible et une rançon vous est demandée pour obtenir la clé de chiffrement afin de pouvoir récupérer vos données. Ce type d'attaque peut être critique, le cas de l'hôpital presbytérien de Hollywood à Los Angeles qui a neutralisé le système pendant 15 jours forçant les responsables à payer la rançon en est la preuve. Celle-ci, initialement fixée à plusieurs millions de dollars, s'est finalement « réduite » à une quinzaine de milliers de dollars. Au-delà du fait que les sauvegardes ne semblaient pas à l'état de l'art dans cet hôpital, il est à noter que le retour en arrière est impossible d'un point de vue purement technique, car les clés de chiffrement utilisées sont incassables dans des délais humainement envisageables (plusieurs centaines d'années de calcul dans le meilleur des cas). Il est donc évident que dans des cas d'infections graves et mettant en jeu des données à forte valeur ajoutée, il n'y a pas d'autre alternative à la sauvegarde que de payer. Ceci, bien entendu, alimente un système de type mafieux bien huilé qui prospère grâce à ce type d'extorsion.

Exemple de mail piégé (reçu le 25/02/2016) :

Facture mobile du 25-02-2016

Free Mobile <freemobile@free-mobile.fr>

Les sauts de ligne en surnombre de ce message ont été supprimés.

Envoyé : jeu. 25/02/2016 15:33
À : Administrateur

Message | Freemobile_0782726443_25-02-2016.zip (2 Ko)

Cher(e) abonné(e),

Veuillez trouver en pièce jointe votre facture mobile du 25-02-2016, d'un montant de 36.18 .

Vous pouvez tout moment désactiver la réception de votre facture par email dans votre espace abonné : http://mobile.free.fr

Sincères salutations.

L'équipe Free

--
Free Mobile - SAS au capital de 365.138.779 Euros - RCS PARIS 499 247 138 - Siège social : 16 rue de la Ville l'Evêque 75008 Paris

Les parades sur ce type d'attaque sont soit physiques avec une interception des pièces jointes dans les mails piégés grâce à des appliances[1] dédiées, soit logiques avec des restrictions de scripts locales sur les machines (navigateurs et outils bureautiques), soit enfin via une sensibilisation accrue des utilisateurs aux risques informatiques et, particulièrement sur ce dernier bien conçu pour attirer ses victimes.

Dans la plupart des cas recensés, il est nécessaire d'effectuer une opération de validation après ouverture du fichier infecté (acceptation de l'exécution d'une macro sur Word ou autre sollicitation), mais le double clic sur une pièce en format.zip (souvent une photo) peut enclencher le processus sans autre forme d'avertissement. Une fois cliqué sur cette approbation ou sur cette pièce jointe, le piège se referme et le virus se propage. Il commence par télécharger un code malveillant et une clé de chiffrement complexe sur un site externe, pour attaquer l'ordinateur. Ensuite, il désactive les sécurités de Windows qui permettraient de revenir en arrière et s'attaque au chiffrement des données accessibles. Par « accessible », on entend l'ensemble des données, y compris celles qui se trouvent sur les lecteurs réseaux. Si au départ, les fichiers ciblés étaient uniquement les fichiers avec des extensions explicitement bureautiques .pdf .doc(x) .xls(x), les nouvelles variantes de ces virus ont un spectre beaucoup plus large et vont jusqu'à chiffrer des fichiers de bases de données. Dans ce cas précis, l'activité s'arrête complètement, car au-delà des simples fichiers de bureautique, ce sont les logiciels métiers qui s'arrêtent et avec eux, l'activité de la collectivité. Les risques en cas de défaut de sauvegarde sont de ne pas pouvoir relancer la production. La perte d'exploitation peut être totale et les conséquences pour la collectivité dures à appréhender.

[1] Voir Glossaire

Exemple du programme malveillant LOCKY et des extensions de fichiers touchées :

.m4u | .m3u | .mid | .wma | .flv | .3g2 | .mkv | .3gp | .mp4 | .mov | .avi | .asf | .mpeg | .vob | .mpg | .wmv | .fla | .swf | .wav | .mp3 | .qcow2 | .vdi | .vmdk | .vmx | .gpg | .aes | .ARC | .PAQ | .tar.bz2 | .tbk | .bak | .tar | .tgz | .gz | .7z | .rar | .zip | .djv | .djvu | .svg | .bmp | .png | .gif | .raw | .cgm | .jpeg | .jpg | .tif | .tiff | .NEF | .psd | .cmd | .bat | .sh | .class | .jar | .java | .rb | .asp | .cs | .brd | .sch | .dch | .dip | .pl | .vbs | .vb | .js | .asm | .pas | .cpp | .php | .ldf | .mdf | .ibd | .MYI | .MYD | .frm | .odb | .dbf | .db | .mdb | .sql | .SQLITEDB | .SQLITE3 | .asc | .lay6 | .lay | .ms11 (Security copy) | .ms11 | .sldm | .sldx | .ppsm | .ppsx | .ppam | .docb | .mml | .sxm | .otg | .odg | .uop | .potx | .potm | .pptx | .pptm | .std | .sxd | .pot | .pps | .sti | .sxi | .otp | .odp | .wb2 | .123 | .wks | .wk1 | .xltx | .xltm | .xlsx | .xlsm | .xlsb | .slk | .xlw | .xlt | .xlm | .xlc | .dif | .stc | .sxc | .ots | .ods | .hwp | .602 | .dotm | .dotx | .docm | .docx | .DOT | .3dm | .max | .3ds | .xml | .txt | .CSV | .uot | .RTF | .pdf | .XLS | .PPT | .stw | .sxw | .ott | .odt | .DOC | .pem | .p12 | .csr | .crt | .key

Dans le cas de déploiement dans l'état de l'art[2], seuls des comptes de services internes à l'application doivent avoir des droits en direct sur les fichiers de bases de données. Malheureusement, certains éditeurs, pour des raisons de coût essentiellement et de manque de sensibilité à la sécurité du développement, font l'impasse sur ces éléments de sécurité. Les risques sont donc accrus lors de tentatives d'infection si les accès aux bases de données se font à partir de comptes non dédiés à l'application elle-même. Le cloisonnement est de rigueur sur ce type d'installation. Là encore, l'export des données et les sauvegardes doivent être faits le plus souvent possible afin de procéder à un éventuel retour en arrière sans perte d'exploitation excessive. La fréquence des sauvegardes est à définir en fonction de la criticité des dossiers.

De même, nombre de failles de sécurité sont liées à des installations « zéro configuration ». Les moteurs de bases de données sont déployés en mode « suivant, suivant… » et il n'y a pas de design autour de l'installation au niveau des comptes de services, qui restent avec des mots de passe par défaut. Or, ces mots de passe sont connus et ces comptes se retrouvent être des failles de sécurité importantes puisqu'il est possible de rebondir[3] sur ces derniers de manière triviale afin d'attaquer le reste du système.

2 Voir Glossaire
3 Voir Glossaire

Les menaces les plus marquantes restent les défauts d'implémentation de sécurité de base dans les collectivités, et surtout celles de petite taille. Nombre de supports de sauvegarde sont de simples disques durs, en permanence branchés sur la machine cible, et quasiment jamais vérifiés. Outre la faible protection du support de sauvegarde, ce dernier reste vulnérable, au même titre que la machine en cas d'infection, de quelque type que ce soit. Sa protection physique n'est pas du tout assurée. Le disque est souvent à demeure et reste branché 24h/24. La solution pour ces petites collectivités qui commencent à être implémentées par certains éditeurs de solutions métier, reste la sauvegarde externalisée. Ce domaine sera évoqué dans la fiche dédiée à la sauvegarde.

Fiche n° 1

LES ACCÈS
DES UTILISATEURS
D'UN SYSTÈME
D'INFORMATION (SI)
(ADMINISTRATEURS,
UTILISATEURS, ÉLUS,
PRESTATAIRES,
STAGIAIRES…)

Fiche n° 1

LES ACCÈS DES UTILISATEURS D'UN SYSTÈME D'INFORMATION (SI) (ADMINISTRATEURS, UTILISATEURS, ÉLUS, PRESTATAIRES, STAGIAIRES…)

Synthèse

La gestion des comptes

- Créer un compte par utilisateur identifié
- Avoir une procédure de départ et d'arrivée pour un agent de la collectivité (création/suppression d'un compte utilisateur, création suppression des boites mails et attribution/restitution des matériels de la collectivité)
- Avoir une procédure d'accès aux différents tiers (maintenance, éditeur, stagiaire,…)
- Avoir une grille des autorisations sur les dossiers informatiques (qui a droit à quoi en lecture, création, modification et suppression)
- Créer des comptes de service pour les tâches d'administration (création des comptes, installations d'applications…)
- Ne pas créer de comptes trop basiques avec des mots de passe triviaux pour ne pas donner de possibilité de rebond dans le système (exemple classique du compte scan sur les copieurs)
- Tenir à jour une cartographie de l'ensemble des utilisateurs avec un privilège supérieur à « utilisateur » (qui a droit à quoi)
- Répertorier les comptes VIP et mettre en œuvre une vigilance accrue sur ces comptes (Elus, directeurs…)
- Interdire l'accès au réseau aux comptes anonymes (non authentifiés)

La gestion des accès physiques

- Chaque matériel vital (serveurs, réseaux, …) de l'infrastructure ne doit être accessible que par les administrateurs
- Les accès à la salle blanche[4] doivent être restreints aux administrateurs et journalisés (repertoriés dans un journal des entrées/sorties).

[4] Salle Serveur

1. La gestion des comptes

L'accès aux données reste quelque chose de très important dans la collectivité. En effet, un cloisonnement correct des droits peut éviter bien des déboires. Dans un premier temps, les différentes personnes ayant accès au réseau informatique doivent être dûment identifiées et leurs droits d'accès clairement exprimés dans un document de synthèse. Cela permet une gestion fine des droits et une meilleure confidentialité des données dans la collectivité. Les différentes personnes utilisatrices du système d'information doivent aussi être sensibilisées à la confidentialité des données qu'elles manipulent. Cela concourt à éviter des divulgations de mots de passe intempestives qui au final ne donnent plus aucune confidentialité à quelque donnée que ce soit. Certaines données peuvent avoir une confidentialité accrue (données RH, médicales, statutaires, comptables…) et doivent faire l'objet d'une attention toute particulière tant sur leur accès que sur leur pérennité. Les connexions anonymes ne doivent pas être autorisées sur les réseaux de production.

Les comptes utilisateurs doivent faire l'objet d'une attention particulière. Une procédure complète doit être déterminée pour l'arrivée d'un agent ou pour son départ. Cette procédure doit aussi exister pour toute autre personne susceptible d'intervenir sur le système d'information (stagiaire, prestataire, intervenant télécom…). Trop de comptes inutiles restent actifs sur les systèmes d'information. Or, ces comptes peuvent être des objectifs d'attaquant pour pouvoir rebondir dans le système et l'attaquer plus en profondeur.

Chaque compte utilisateur ne doit pas comporter plus de privilèges que nécessaire. Un utilisateur ne doit pas être, sauf contrainte technique impérative, administrateur de son poste. En cas de compromission, un processus malveillant arrive ainsi avec des droits peu étendus et ne peut pas « facilement » se propager dans le système car ses droits ne lui permettent que des actions très limitées. A contrario, un utilisateur administrateur de son poste pourra voir la compromission de son poste avoir beaucoup plus de conséquences car le processus malveillant a les pleins droits sur la machine dans son entier. Le système peut donc être corrompu de manière totale et avoir des conséquences sur le SI dans son entier.

Les accès des administrateurs doivent être très contrôlés et très cadrés eux aussi car ce sont les détenteurs des clés du système d'information. Les administrateurs doivent avoir des comptes distincts avec des droits différents et des mots de passe personnels. Ils ne doivent, en aucun cas, être similaires pour ne pas corrompre l'ensemble du système en cas de compromission d'un compte.

Chaque administrateur doit se voir attribuer des droits en fonction de sa mission au sein du système. Les comptes administrateurs ne doivent, en aucun cas, servir à autre chose qu'administrer les systèmes ou les équipements. Aucun de ces comptes ne doit servir sur une machine pour aller sur Internet ou pour prélever ses messages personnels. Ces comptes sont généralement critiques pour le fonctionnement du SI, il est donc de bon ton de ne pas les exposer inutilement. Une compromission via un compte utilisateur peut être gérable si la segmentation des droits est correcte et que les sauvegardes sont opérationnelles. La compromission d'un compte administrateur est beaucoup plus complexe à gérer car on doit partir du principe que le système d'information dans son entier est corrompu. Un document de suivi des droits des administrateurs doit être tenu à jour régulièrement pour avoir une image la plus fidèle possible de la cartographie des droits de ces derniers. Cela permet aussi d'effectuer des contrôles et des vérifications sur l'activité des comptes.

Les comptes VIP restent assez complexes à gérer. Des demandes de droits étendus (administrateur du poste) sont souvent associées à ce type de compte. Les accès sont généralement eux aussi étendus (plus de dossiers en accès en fonction du niveau de responsabilité dans la collectivité), ce qui en fait des comptes critiques et donc à surveiller. Ces comptes sont souvent plus vulnérables que les autres car très fréquemment embarqués sur des terminaux portables (voir fiche sur le BYOD). Toute compromission d'un de ces comptes doit entraîner, de la part des services en charge de l'informatique, une réponse immédiate et proportionnée à l'enjeu. Si un doute survient sur la validité de la personne qui consulte les mails et/ou les fichiers, une mesure de blocage immédiate du compte doit être engagée. Il faut ensuite avertir la personne potentiellement victime de malveillance et le cas échéant lui donner la procédure de retour à la normale.

2. La gestion des accès physiques

Les accès physiques sont à contrôler de la même manière que les accès logiques. Seules les personnes ayant besoin, pour des raisons de maintenance, d'avoir accès aux éléments physiques du Système d'information doivent pouvoir y accéder. Les accès aux locaux critiques doivent être soumis à authentification et journalisés afin de pouvoir revenir sur un éventuel problème de sécurité.

Sur ce concept, personne d'autre que des administrateurs ne doit pouvoir accéder à la salle blanche et aux locaux techniques hébergeant les éléments du réseau.

Fiche n° 2

LES MOTS DE PASSE

Fiche n° 2
LES MOTS DE PASSE

Synthèse

- Chaque accès, que ce soit à un compte ou à une application, doit avoir un mot de passe différent
- Il doit remplir des critères de longueur et de complexité
- Il ne doit pas être stocké dans autre chose qu'une application sécurisée dédiée
- Il ne doit jamais être généré en ligne
- Ne jamais conserver des mots de passe par défaut
- Il doit être changé avec une occurrence adaptée à sa criticité

Que ce soit dans le monde professionnel ou personnel, le mot de passe est le principal rempart contre la plupart des menaces, il protège nos comptes et nos données. Il n'est pas assez considéré et traité au mieux comme un élément de sécurité et au pire, comme une contrainte insurmontable. L'ensemble des systèmes d'information modernes repose sur des systèmes d'authentification par mot de passe, les systèmes d'authentification par carte à puce et autres méthodes physiques n'étant pas encore très répandus. La contrainte du mot de passe est multiple, il doit répondre à certaines normes en fonction de son utilisation (obligation de complexité sur certains systèmes), il doit être changé de manière régulière et ne doit pas servir à plusieurs accès. Dans le cas d'une application nouvelle ou d'un équipement neuf, le premier réflexe doit être de changer le mot de passe par défaut.

La complexité d'un mot de passe reste, au regard de l'utilisateur normal, une contrainte. Elle représente un effort à faire périodiquement et l'utilisateur n'en voit souvent pas l'intérêt. La question qui revient le plus souvent reste « à quoi ça sert, nous n'avons rien de secret ». Cela dénote deux choses. La première est une méconnaissance des implications liées à une compromission de poste et la seconde, un manque de sensibilité au traitement des informations à caractère privé de la collectivité, quelle qu'elle soit.

La collection des 25 mots de passe les plus utilisés dans le monde en 2015 reste édifiante :

1 - 123456
2 - password
3 - 12345
4 - 12345678
5 - qwerty
6 - 123456789
7 - 1234
8 - baseball
9 - 696969
10 - football
11 - welcome
12 - 1234567890
13 - abc123
14 - 111111
15 - 1qaz2wsx
16 - dragon
17 - master
18 - monkey
19 - letmein
20 - login
21 - princess
22 - qwertyuiop
23 - solo
24 - passw0rd
25 - starwars

Le choix du mot de passe est donc capital. Il existe un certain nombre de règles simples permettant de créer des mots de passe robustes. Aujourd'hui, on estime qu'un mot de passe dit « robuste » doit avoir douze caractères avec un mélange de minuscules, majuscules, chiffre et caractères spéciaux et il doit être sans lien personnel avec l'utilisateur (à bannir le nom du chat ou la date de naissance des enfants ou du conjoint) et sans lien non plus avec l'entité pour laquelle vous évoluez. Deux solutions restent assez fiables pour créer un mot de passe et conserver un moyen mnémotechnique de s'en souvenir :

- La méthode de substitution phonétique ; exemple : « Je suis un indien de l'Utah » donne : J$ui11Di12L'utA.
- La méthode de la première lettre/phonème d'une citation ou d'une phrase ; exemple : « Ce qui est incompréhensible, c'est que le monde soit compréhensible ». (A. Einstein) : cQé1c'EqLm$c.

La génération sur internet d'un mot de passe est à proscrire pour une raison évidente, la personne qui vous le génère peut au mieux vous avoir mis en ligne un outil pratique (fort peu probable) au pire, le stocker pour l'exploiter ou le revendre à un tiers attaquant.

Le changement de mot de passe contribue aussi à la sécurité des comptes. Il est recommandé de les changer tous les 90 jours. Pour des raisons évidentes, il faudra faire la part des choses entre les comptes que l'on considère comme critiques et ceux qui le sont moins, et y adapter la fréquence (ou occurrence) de changement.

Le stockage des mots de passe reste un problème. Il faut en avoir un par application (messagerie, banque en ligne, Facebook, compte PayPal…) et s'en souvenir. S'ils respectent des normes de complexité citées ci-dessus, cela peut vite devenir impossible. L'envoi de mails avec des mots de passe pour les stocker et s'en souvenir est à proscrire. Les stocker dans son navigateur est très dangereux car pour l'exemple de Firefox, il suffit de trois clics de souris pour les faire apparaître en clair. Il ne faut pas non plus générer un fichier avec l'ensemble de vos mots de passe. Si ce dernier est frauduleusement acquis, tous vos comptes sont vulnérables. La solution peut donc passer par des petites solutions de « coffres à clés ». La plus connue, et celle qui est recommandée par l'ANSSI, est Keepass un petit logiciel qui va chiffrer de manière forte l'ensemble de vos logins/mots de passe avec en entrée un seul mot de passe dont, cette fois, il faudra se souvenir. Il est disponible à l'adresse suivante : http://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/.

Fiche n° 3

LES SAUVEGARDES

Fiche n° 3
LES SAUVEGARDES

Synthèse

- Bien identifier les données à sauvegarder
- Etablir un plan de sauvegarde en fonction de la rétention souhaitée
- Définir les cibles pour les sauvegardes en regard de la volumétrie induite (NAS, bande, sauvegarde déportée…)
- Donner une possibilité d'externaliser les données les plus critiques (choix direction)

La sauvegarde est la pierre angulaire de la reprise d'activité en cas de sinistre. Quelle que soit la nature de la perte de données, elle est la seule alternative pour un retour à la normale avec une perte minimale d'exploitation. Les plans de reprise et de continuité d'activité s'appuient sur des sauvegardes correctes et pérennes. Elle doit être obligatoirement réfléchie en amont et planifiée de manière rigoureuse. La rétention doit être décidée en fonction de la criticité des données de la collectivité préalablement identifiée comme telle et les délais légaux de conservation des données.

Elle doit permettre la restauration d'un état antérieur du SI après une suppression accidentelle de données (par exemple suite à une erreur d'un utilisateur ou d'un exploitant), une altération de données ou programmes informatiques (par exemple suite à une infection virale, à une panne d'un composant physique du Système d'Information, ou encore à un incident environnemental dans un Datacenter).

Le plan de sauvegarde doit être établi d'après les critères ci-dessus. Les supports doivent aussi être choisis en fonction de différents critères. Les bandes magnétiques, les supports sur NAS[5], les sauvegardes déportées.

[5] NAS : Serveur de fichiers

Le choix des solutions de sauvegarde présente également :

des enjeux opérationnels d'exploitation du système d'information :

- les capacités de stockage nécessaires à la sauvegarde peuvent varier selon les modes de sauvegarde retenus (par exemple : sauvegarde totale ou partielle, sauvegarde différentielle entre deux sauvegardes afin de limiter la quantité de données sauvegardées à chaque fois),
- Les contraintes opérationnelles sur les applications peuvent être différentes selon que la sauvegarde est réalisée à chaud (applications en fonctionnement pendant le déroulement de la sauvegarde) ou à froid (applications arrêtées lors du déroulement de la sauvegarde),
- les délais acceptables de restauration pour des données à forte volumétrie peuvent justifier des techniques spécifiques de sauvegarde.

des enjeux financiers :

Le coût de la sauvegarde est fortement dépendant du niveau de service attendu (fréquence des sauvegardes, durée de rétention…). Il est donc important de choisir les solutions de sauvegarde adaptées et de définir des processus associés. Ceci afin de répondre aux enjeux de sécurité mais également financiers dans un souci d'efficience économique en cohérence avec le besoin opérationnel de la collectivité.

Le choix d'une sauvegarde déportée doit être réfléchi de manière à la mettre en œuvre en sécurité. La pérennité et la sécurité doivent être la préoccupation première du responsable de la sauvegarde. Le chiffrement à la source est recommandé si les données sont hébergées à l'extérieur. Cette solution doit être envisagée quand les données ne peuvent pas être stockées ailleurs que dans la pièce de production. Les mises en coffre-fort des bandes magnétiques peuvent prémunir d'un vol physique des données, mais contrairement aux idées reçues, ne peuvent résister à un incendie. Elles sont essentiellement faites de plastique qui fond et se déforme à la chaleur. Ces supports, bien que « protégés » seraient donc, en cas d'incendie, inutilisables pour une restauration de données.

Différentes normes régissent les systèmes de sauvegarde, elles sont issues des bonnes pratiques en matière de SSI ainsi que de documents de référence :

Les recommandations de la fiche technique sur la sauvegarde de l'ANSSI : « Fiche technique relative à la sauvegarde ».

Les bonnes pratiques en matière de sauvegarde identifiées dans :

- la norme ISO/CEI 27002 - « Code de bonnes pratiques pour la gestion de la sécurité de l'information »,
- La norme ISO 22301 – « Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences »,
- Les bonnes pratiques relatives aux sauvegardes de données à caractère personnel publiées par la CNIL : « Guide Mesures pour traiter les risques sur les libertés et la vie privée »,
- Le guide pour réaliser un plan de continuité d'activité (SGDN).

Fiche n° 4

LES PROTECTIONS PHYSIQUES

Fiche n° 4
LES PROTECTIONS PHYSIQUES

Synthèse

- Isolation des éléments avec contrôle d'accès
- Mise en place des salles avec les bonnes pratiques
- Mettre dans le projet les acteurs du SI pour la création/modification des lieux d'hébergement

Les protections physiques à mettre en œuvre sur un système d'information doivent être en rapport avec l'importance de ce dernier. Certains sites hébergeant des données restent moins critiques que d'autres, par exemple un site autonome dans une collectivité avec peu de données et une criticité faible. Mais ce qui est considéré comme le cœur du système doit toujours être protégé de manière adéquate. Beaucoup de systèmes d'information se retrouvent confinés dans des pièces non protégées au niveau des accès, sans élément de réfrigération pour assurer une température de fonctionnement optimale et sans aucun contrôle d'accès (voire même dans des pièces de passage). Cela représente un risque non négligeable d'atteinte physique au système. Les atteintes peuvent être volontaires (dans un but de nuisance ou de captation d'informations), environnementales (problèmes électriques, inondation, incendie) ou involontaires, (chocs, renversement de liquides, arrachage accidentel de câbles…). Pour se prémunir de ce type d'incidents, il faut cloisonner les différents éléments du système d'information pour le prémunir contre les accès frauduleux ou malveillants et anticiper les « accidents » quotidiens (café renversé, coupure électrique, erreur de manipulation…).

Toutes ces protections sont souvent difficiles à mettre en œuvre sur des éléments déjà constitués. Mais cela doit être un axe de réflexion majeur lorsqu'il s'agit de création en bâtiment neuf ou en rénovation. Force est de constater que cette mise en place est rarement prise en compte lors de la gestation de ces projets. Certains aménagements sont même catastrophiques lorsqu'ils ne sont pas mis en œuvre avec des personnes sensibilisées à la mise en place de salles hébergeant des éléments de système d'information.

Dans certains cas extrêmes, le système d'information peut même être mis en danger par ignorance des concepts de base de la sûreté de fonctionnement. Un exemple récent en audit a permis de trouver une « salle blanche » remisée dans un placard avec une climatisation. Sur ce cas, en plus d'être confiné et techniquement complètement inaccessible, l'ensemble du système d'information (matériel de production et sauvegarde !) était surplombé par des canalisations en activité (adduction et évacuation d'eau). La moindre fuite donnerait dans ce cas une perte totale d'exploitation avec peu de chance de restauration.

Il est donc nécessaire de faire intervenir, dans tous les cas d'aménagement ou de déplacement de salle informatique, les acteurs du SI (service informatique, DSI, RSSI ou prestataire en gestion).

Fiche n° 5

L'INFRASTRUCTURE
SANS FIL (WIFI)

Fiche n° 5
L'INFRASTRUCTURE SANS FIL (WIFI)

Synthèse

- Bien définir le périmètre d'utilisation
- Journaliser et filtrer tous les accès
- Dans la mesure du possible, séparer les point d'accès sans fil du réseau de production
- Penser à changer les clés de chiffrement régulièrement
- Ne pas laisser des accès ouverts inutilement

Une infrastructure sans fil présente dans une collectivité, reste souvent un maillon faible de la sécurité. Entre des clés de chiffrement trop simples ou accessibles (étiquette sur un point d'accès, noté sur un écran ou en mémoire dans tous les portables locaux) et des utilisateurs peu sensibilisés, il est complexe d'établir une sécurité correcte sur ces éléments du réseau. Il faut distinguer trois usages distincts des connexions Wifi dans une collectivité.

La première est un accès libre au public qui doit être géré de manière très rigoureuse en ce qui concerne la trace et les accès. La mise en place d'un portail dit captif[6] est souvent une solution clé en main pour la mise en production d'un tel environnement. Ce réseau doit être obligatoirement isolé du réseau de production. En cas de compromission des accès, la sécurité des données de la collectivité ne serait pas menacée. Le portail captif est positionné en coupure entre l'accès Internet et le réseau de consultation. Il permet d'authentifier les usagers, de contrôler les accès, de tracer les connexions effectuées, de protéger le réseau de consultation. Les éléments traditionnels d'un portail captif sont : une passerelle d'interception, un serveur d'authentification et une base de données usagers.

6 Une solution permettant d'authentifier et de tracer l'utilisateur du wifi dans un lieu public

La seconde est un accès aux élus ou visiteurs d'une collectivité avec uniquement un besoin de connexion internet. Dans ce cas, le traitement est différenciable en fonction du besoin. Si le besoin est essentiellement pour les extérieurs, un traitement identique à une connexion d'accès publique doit être appliqué. S'il est exclusivement destiné en interne mais pour de la consultation internet (smartphone, tablettes…), le réseau Wifi devra là aussi être mis en place avec du filtrage et de la journalisation[7] mais le portail captif, qui reste malgré tout assez contraignant, ne sera pas de mise. Le réseau devra être là encore isolé du réseau de production et avoir une connexion Internet propre à cet usage. D'autre part, la clé de chiffrement devra changer régulièrement et le service WPS (appairage automatique d'un terminal sans fil avec le point d'accès en appuyant sur un simple bouton) systématiquement désactivé sur les point d'accès. Au mieux, ces points d'accès devront bénéficier d'une gestion centralisée pour permettre une meilleure maîtrise de cette infrastructure sans fil. Là encore, en cas de problème au niveau de l'intégrité de la connexion sans fil, les données du réseau de production ne seraient pas impactées.

La troisième est un accès sans fil au réseau de production de la collectivité. Le niveau de sécurité doit alors être bien plus élevé. En effet, cette fois, toute intrusion sur le réseau sans fil permettrait d'avoir un accès direct aux données. L'infrastructure doit donc être déployée avec des technologies de sécurisation supplémentaires. La norme IEEE 802.1X a été mise au point pour l'authentification des utilisateurs sur un réseau, filaire ou non, à l'aide d'un serveur dédié. Le fonctionnement du protocole EAP (utilisé pour les accès au réseau) est basé sur l'utilisation d'un contrôleur d'accès, chargé d'établir ou non l'accès au réseau pour un utilisateur. Le contrôleur d'accès est un simple garde-barrière servant d'intermédiaire entre l'utilisateur et un serveur d'authentification, il ne nécessite que très peu de ressources pour fonctionner. Dans le cas d'un réseau sans fil, c'est le point d'accès qui joue le rôle de contrôleur d'accès.

Le serveur d'authentification permet de valider l'identité de l'utilisateur, transmis par le contrôleur réseau, et de lui renvoyer les droits associés à son profil utilisateur. De plus, un tel serveur permet de stocker et de comptabiliser des informations concernant les utilisateurs afin, par exemple, de pouvoir fournir des preuves de connexions sur requête judiciaire.

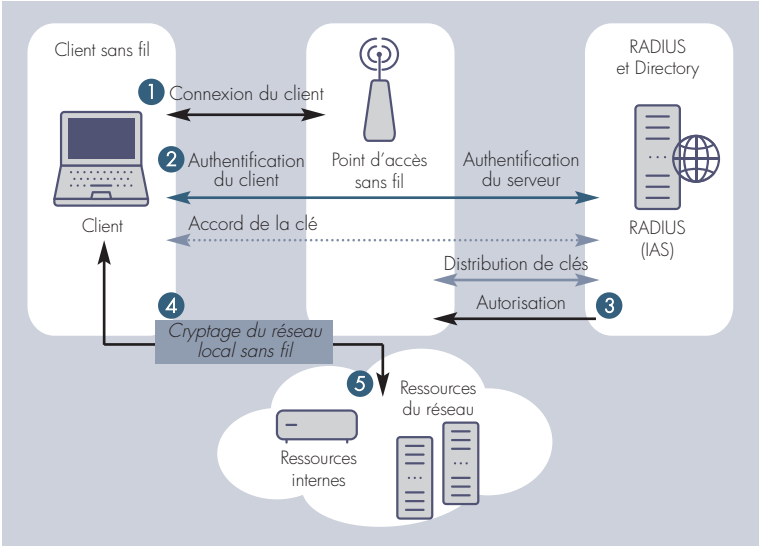
[7] L'ensemble des traces laissées par des utilisateurs sur internet (adresses de pages, heures d'utilisation,…)

La plupart du temps, le serveur d'authentification est un serveur Remote Authentication Dial In User Service (RADIUS), un serveur d'authentification standard défini par les RFC 2865 et 2866[8], mais tout autre service d'authentification peut être utilisé.

Outre l'authentification des utilisateurs, le standard 802.1x est un support permettant de changer les clés de chiffrement des utilisateurs de manière sécurisée, afin d'améliorer la sécurité globale.

La définition de plages horaires d'utilisation peut aussi contribuer à la sécurité de l'infrastructure sans fil. En effet, si les points d'accès sont « fermés » en dehors des plages habituelles d'utilisation, il est plus compliqué pour une personne souhaitant s'introduire dans le réseau, d'être discrète et d'opérer à proximité des points d'accès, la nuit par exemple.

Schéma explicatif de l'authentification forte par serveur RADIUS :



[8] RFC : Request For Comment / Références Techniques Informatiques

Fiche n° 6

LES TERMINAUX PORTABLES
(ORDINATEUR PORTABLE,
SMARTPHONE
ET TABLETTE)

Fiche n° 6
LES TERMINAUX PORTABLES (ORDINATEUR PORTABLE, SMARTPHONE ET TABLETTE)

Synthèse

- Attention à l'usage des équipements personnels (BYOD)
- Ne jamais se séparer de son smartphone
- Mettre en place une politique d'authentification forte avec effacement de données
- Adopter des mots de passe robustes
- Identifier les applications nécessaires et bloquer les autres
- Chiffrer les données de tous les appareils mobiles
- Donner la possibilité à l'administrateur d'effacer les données à distance
- Ne jamais brancher un terminal mobile sur une station de travail autre que celle de l'employeur
- Ne jamais brancher de clef USB non validée sur les terminaux portables

Aujourd'hui, l'ensemble des acteurs de nos collectivités possède un ou plusieurs terminaux portables. Cette prolifération n'est pas sans conséquence sur la possibilité de voir fuiter des données. La sécurisation de ces terminaux reste souvent l'apanage de son propriétaire. Dans ces conditions, nombres d'informations échappent aux administrateurs du réseau et à l'administrateur en charge de la sécurité. Pourtant, ces terminaux regorgent d'informations, contacts, e-mails, documents, photos, données de localisation… Ils vont sur Internet sans être, pour la plupart du temps, limités sur ce qui peut être consulté et servent autant dans la sphère privée que professionnelle. Ces terminaux, s'ils sont fournis par l'employeur, peuvent être maîtrisés grâce à des outils de gestion centralisés permettant d'établir des politiques de sécurité. S'ils sont la propriété de son utilisateur et utilisés à des fins professionnelles, ils prennent la dénomination de Bring Your Own Device (BYOD) = Apporter vos appareils personnels. Le principal défi dans ce dernier cas est de scinder la partie privée de la partie professionnelle et exposée. Pour exemple, les smartphones, de quelque marque qu'ils soient, sont de plus en plus la cible de tentative de corruption dans le but de récupérer un maximum d'informations de la part de l'utilisateur (comptes mail, mots de passe d'application, récupération de la liste des contacts, récupération des sms…). Ces corruptions de données peuvent avoir lieu à l'insu de son utilisateur ou involontairement par sa faute.

La perte d'un smartphone n'est pas rare (aux États-Unis, il se perd 113 smartphones à la minute[9], ce qui peut s'avérer catastrophique en termes de perte de données si le smartphone n'est pas du tout protégé).

L'ANSSI fut longtemps ouvertement opposée à cet usage des BYOD. Son nouveau directeur est plus nuancé et souhaiterait orienter les acteurs vers le CYOP (choose your own device) grâce auquel l'employeur propose à ses employés une sélection restreinte de terminaux certifiés. La CNIL n'est pas très ouverte sur cette solution car elle pose un certain nombre de questions en ce qui concerne la mise à disposition d'objets personnels pour l'activité professionnelle. Elle a d'ailleurs émis des recommandations en ce sens dans un article invitant à la limitation stricte de ces pratiques[10]. En effet, il est impossible pour un employeur de limiter les accès aux informations et aux données personnelles d'un employé sous prétexte que le terminal en question est utilisé à des fins professionnelles.

Quelques mesures sont à prendre pour sécuriser les terminaux portables. Rien n'est infaillible au niveau de la sécurité mais ces mécanismes de défense mis en place feront renoncer la plupart des « trouveurs » de smartphone, ordinateur et autre tablette qui se contentent généralement de les formater pour pouvoir les revendre.

Pour la famille des BYOD, il faut, pour leurs utilisateurs, chiffrer les téléphones et les supports mémoire associés (carte SD). Cela permet, en cas de perte ou de vol, de ne pas accéder aisément aux informations du terminal incriminé. L'identification à l'ouverture doit être autre chose qu'un simple doigt qui glisse sur un écran (encore très fréquent sur des smartphones de personnes détentrices de données critiques). Accepter des contraintes de sécurité telles que l'effacement des données du téléphone après x tentatives manquées pour s'identifier, un mot de passe fort et une sauvegarde régulière des données de l'appareil. Enfin, le plus compliqué, la sensibilisation des utilisateurs à la sécurité de leurs données. Le sacrosaint « je n'ai rien à cacher, je n'ai pas de secret » ne doit plus avoir cours. Tous les utilisateurs se doivent de protéger, au-delà de leur vie privée qui leur incombe, leurs données professionnelles si elles viennent à être présentes pour une raison ou pour une autre sur leur matériel personnel. Il est a noté la très grande dangerosité des appareils dits « rooté ». En effet, ces derniers n'ont aucun frein sur l'installation de logiciels classiques ou malveillants puisque les verrous ont été enlevés pour prendre le contrôle total de l'appareil et s'affranchir de la validation des stores officiels de diffusion d'applications mobiles.

[9] Source : « What's the Worst U.S. City for Smartphone Theft ?, Mashable »
[10] https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques

Mais si les verrous ne sont plus là pour l'utilisateur qui est donc administrateur de son/sa smartphone/tablette, ils ne sont plus là non plus pour les applications malveillantes qui vont pouvoir s'installer sans aucun frein. Cette pratique reste marginale, mais elle peut corrompre l'intégrité d'un réseau et de ses données par ignorance des risques encourus par ce type de pratique.

La protection des terminaux mis à disposition par l'employeur est plus aisée. Au-delà du fait qu'il faut, là aussi, sensibiliser les gens à la sécurité des données, il y a la dimension outil de travail qui rentre en compte. Les différentes contraintes inhérentes à la sécurité des unités portables peuvent être imposées par l'employeur puisqu'il s'agit de matériel lui appartenant. Dans ce cas, il est préconisé de bien choisir les terminaux en fonction des exigences de sécurité que l'on a. Tous ne se valent pas et certains sont complètement dédiés aux professionnels. Cela peut permettre une gestion centralisée, une limitation des accès en fonction du besoin de sécurité, une mise en place de stratégie de restriction d'installation sur les différents stores d'application. Une infrastructure autonome à la collectivité peut même être créée pour gérer les mises à jour des terminaux et leur sécurité. Les autres règles de base doivent aussi être mises en place. Pas de connexion sur des équipements autres que ceux de l'employeur, chiffrement des données systématique, possibilité d'effacement à distance du téléphone ou de la tablette, mise en place de mots de passe forts avec un blocage temporel de plus en plus long en fonction des échecs successifs, et un effacement au bout d'un nombre de tentatives de connexions erronées déterminé par le responsable sécurité. Tout comme pour un ordinateur classique, il ne faut pas brancher de clé USB qui ne soit pas certifiée comme correcte par le service informatique.

Fiche n° 7

LES CLÉS USB ET AUTRES SUPPORTS FLASH

Fiche n° 7
LES CLÉS USB ET AUTRES SUPPORTS FLASH

Synthèse

- Utiliser avec parcimonie
- Les destiner à une utilisation très ciblée et ne pas y déroger
- Chiffrer les données si elles s'avèrent d'importance pour leur détenteur
- Ne jamais passer un support de ce type de la sphère privée à celle du travail

Les clés USB et autres supports de mémoire de type flash (mémoire de stockage sans pièces mécaniques) sont de plus en plus utilisés dans notre environnement personnel ou professionnel. Quel que soit leur usage (carte mémoire d'appareil photo, carte d'extension de mémoire téléphone, clé USB) ces supports sont de plus en plus volumineux en termes de données. Cependant, ces différents éléments sont des points de vulnérabilité pour les systèmes d'information. En effet, ils sont indifféremment branchés sur des stations professionnelles dont la sécurité est garantie par les bonnes pratiques mises en place sur le système d'information, que sur des stations personnelles dont la sécurité est pour le moins aléatoire en fonction du niveau d'expertise personnel du détenteur de la machine et de sa sensibilité à la sécurité informatique. Il est donc évident que cette dualité est dangereuse à plus d'un titre. Un média amovible utilisé sur un poste infecté peut potentiellement corrompre l'ensemble des éléments fiables d'un système d'information. Les menaces venues de l'intérieur sont beaucoup plus difficilement identifiables par les administrateurs car elles relèvent très souvent du comportement humain et de sa faculté à vouloir contourner les règles.

La fragilité de ces éléments n'est plus à démontrer, nombre de ces supports sont détruits par inadvertance. Une clé en façade d'un poste de travail est très vulnérable physiquement. En effet, un simple choc latéral peut l'endommager de manière définitive. Dans ce cas, la perte de données est totale avec aucune chance de retour arrière, sauf à faire appel à un laboratoire spécialisé, ce qui est très coûteux.

Les supports mémoire et les clés USB en particulier peuvent être des vecteurs de propagation de logiciels malveillants. Ces éléments sont souvent en exécution automatique lorsqu'ils sont insérés dans un ordinateur, ce qui en fait un média idéal pour infecter un poste de travail à l'insu de son propriétaire. Une des méthodes préférées des pirates pour infecter des postes est la dissémination de clés USB, infectées par du code malveillant, de manière aléatoire. Elles sont mises en évidence de manière volontaire afin d'être trouvées « par hasard », branchées à un ordinateur pour en voir le contenu et surtout pour propager un virus ou tout autre outil de captation d'informations. Cette technique a en partie été utilisée pour déployer le virus STUXNET qui a servi au sabotage des centrifugeuses Iraniennes d'enrichissement d'uranium.

Ces supports sont de plus en plus petits avec des capacités de plus en plus grandes. De plus en plus d'informations sont concentrées dans des éléments de plus en plus faciles à égarer. Il est donc de bon ton de ne mettre que des informations peu importantes ou chiffrées sur ce type de support afin que leur perte éventuelle n'engendre pas de conséquences importantes pour leur propriétaire.

Le bon usage des supports de ce type est d'être prudent avec leur manipulation, leur destiner un usage unique et ne pas y déroger. Ne pas mettre les éléments en lecture automatique sur les postes de travail. Considérer une clé USB inconnue comme potentiellement dangereuse pour la sécurité de votre réseau et la traiter comme telle. Une clé inconnue peut être testée uniquement sur une station blanche (station autonome déconnectée du réseau, de l'Internet et généralement avec un système linux).

Fiche n° 8

LE SHADOW IT (TECHNOLOGIE INFORMATIQUE FANTÔME)

Fiche n° 8
LE SHADOW IT (TECHNOLOGIE INFORMATIQUE FANTÔME)

Synthèse

- Côté gestionnaire du système d'information : cerner les besoins des utilisateurs pour mettre des solutions validées, en adéquation avec leur besoin, à leur disposition
- Côté utilisateur : remonter les besoins pour l'accomplissement des missions avec le plus de clarté possible pour être compris par les acteurs du système d'information
- Ne pas restreindre de manière trop drastique tous les usages des ressources IT au sein du SI pour ne pas générer « d'envies de contournement »

Derrière cette dénomination barbare se cache un phénomène complexe à gérer au quotidien pour un administrateur, à savoir des éléments déployés par les utilisateurs sans en référer à la DSI. Cela va de l'utilisation des BYOD (voir fiche n° 6) à des choses plus problématiques dans le contrôle des données générées par la structure, comme la mise en place d'un « cloud » non répertorié[11], le déploiement de matériel non référencé, l'intervention d'informaticiens extérieurs à la structure et le plus important en termes de chiffres les macros Excel non validées. Cette liste est non exhaustive et tous les jours, les méthodes de communication permettent de nouvelles possibilités de développer ce phénomène. A ce titre, une partie de l'information échappe complètement au gestionnaire du système d'information, les sauvegardes ne sont plus assurées et la potentialité de perdre des données augmente avec le nombre d'utilisateurs du service « hors cadre ». Les logiciels non répertoriés sont aussi une composante importante du shadow IT, ils répondent à un besoin immédiat de certains utilisateurs et représentent un risque dans le sens où la solution n'a pas été testée ni approuvée en termes de sécurité et génère des données non contrôlées. Le retour arrière sur des applications de ce type est quasiment impossible, les données n'étant pas répertoriées officiellement, elles ne sont donc pas intégrées dans le cycle de sauvegarde du système d'information. Malgré tout, cet état de fait est révélateur d'un besoin des utilisateurs qui n'est pas forcément toujours pris en compte par la DSI.

[11] Circulaire du 5 avril 2016 sur l'informatique en nuage

Le temps des utilisateurs passifs des SI est révolu, la culture numérique prenant de plus en plus d'ampleur. Les méthodes de substitution pour un outil manquant sont de plus en plus accessibles à ces derniers qui n'hésitent plus à sauter le pas de l'installation.

Malgré tout, les dangers liés à cette pratique sont bien présents. Dans le cadre de l'exploitation d'un logiciel tiers non validé, la perte de données est une menace constante. Ces logiciels sont souvent installés sur un poste de travail qui n'a pas de moyen de sauvegarde et ne présente aucune sécurité accrue de fonctionnement, contrairement aux serveurs. La panne technique peut donc être fatale aux données générées par l'application. Dans le cadre d'adjonction de matériel non répertorié, le risque est tout aussi grand. Il passe de la mauvaise installation/utilisation du matériel à un usage inapproprié qui pourrait mettre en danger le SI. Dans le cadre des macros Excel, elles peuvent aller à l'encontre de la politique de sécurité qui consiste par défaut à les désactiver pour éviter des attaques par ce biais. Elles peuvent aussi être plus pernicieuses en générant elles-mêmes une faille sur une mauvaise implémentation. Dans le cadre des BYOD, un smartphone peut très bien être utilisé en modem pour contourner des règles jugées trop restrictives. Dans ce cas précis, l'exposition est maximale par rapport à la sécurité car l'adjonction de ce point d'entrée Internet non géré et surtout non contrôlé augmente terriblement la surface d'attaque.

Les exemples ne manquent pas entre les BYOD et toutes les nouvelles technologies de communication et de partage. La solution reste de travailler en étroite collaboration les uns avec les autres. L'expression des besoins doit être faite en temps et en heure de la part des utilisateurs, et le gestionnaire du SI doit s'efforcer d'y répondre de son côté dans la mesure du possible. Cela reste la meilleure des manières de ne pas avoir besoin de recourir à des éléments externes au SI. Malgré tout, le gestionnaire doit rester vigilant et en écoute pour essayer de détecter tout élément étranger à son réseau pour pouvoir, le cas échéant, prendre des mesures face au déploiement de tels dispositifs.

Fiche n° 9

L'INFORMATIQUE
DANS LES ÉCOLES

Fiche n° 9
L'INFORMATIQUE DANS LES ÉCOLES

Outre le fait que le numérique entre de plus en plus dans toutes les tranches de la scolarité des enfants, des problèmes de mise en place se posent. Pour mettre de l'informatique dans une école, il est souvent plus simple de mettre en place un système à base de wifi plutôt qu'à base de solution filaire qui nécessite un câblage coûteux. Le côté pratique du wifi n'est plus à démontrer mais en ce qui concerne les écoles, il est devenu une source d'inquiétude en matière de santé publique. Les ondes émises par les appareils délivrant du wifi ne sont pas, pour le moment, sans poser de questions quant à la conséquence d'une exposition des enfants à leur rayonnement.

Dans ce cadre, le gouvernement a dû légiférer pour trouver un point d'équilibre entre l'émission potentielle d'ondes nocives et le côté fonctionnel du wifi dans les écoles. Le texte encadrant ces normes est disponible ici : https://www.legifrance.gouv.fr/eli/loi/2015/2/9/DEVX1402671L/jo/texte.

En substance, elle interdit tout fonctionnement d'appareils radioélectriques dans l'environnement des enfants de moins de trois ans (article 7, paragraphe 1) : « Dans les établissements mentionnés au chapitre IV du titre II du livre III de la deuxième partie du code de la santé publique, l'installation d'un équipement terminal fixe équipé d'un accès sans fil à internet est interdite dans les espaces dédiés à l'accueil, au repos et aux activités des enfants de moins de trois ans ».

Elle autorise le wifi dans les écoles sous cette forme (article 7, paragraphe II) : « Dans les classes des écoles primaires, les accès sans fil des équipements mentionnés à l'article 184 de la loi n° 2010-788 du 12 juillet 2010[12] portant engagement national pour l'environnement, installés après la publication de la présente loi, sont désactivés lorsqu'ils ne sont pas utilisés pour les activités numériques pédagogiques. ».

12 https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=4D2ADA2BD7235ACC8D4520A1E1C09189.tpdila19v_2?idArticle=LEGIARTI000030216714&cidTexte=LEGITEXT000022472766&dateTexte=20160419

Elle oblige à une information en conseil d'école pour toute nouvelle installation d'appareils wifi dans les écoles (article 7, paragraphe 3) : « Dans les écoles primaires, toute nouvelle installation d'un réseau radioélectrique fait l'objet d'une information préalable du conseil d'école. »

D'autre part, la protection radioélectrique est une chose mais la protection des élèves, quels qu'ils soient, vis-à-vis de contenus inappropriés sur Internet en est une autre. Des éléments de filtrage d'URL[13] doivent être mis en place pour pallier cette éventualité. Différents systèmes de filtrage ont été décrits dans la fiche n° 11 de ce présent guide.

Cependant, en ce qui concerne les écoles, une solution « presque clé en main » existe sous la forme d'un serveur appelé AMON. Ce serveur, dont les sources sont disponibles gratuitement auprès de l'éducation nationale, après signature d'une convention, permet un filtrage des URL avec une mise à jour très régulière des listes de filtrage. Il répond aussi aux différents critères de rétention des logs (journaux) en ce qui concerne la consultation des pages internet. Reste à la charge de la collectivité, l'acquisition des machines support et la prestation d'installation. Ensuite, les éléments de dysfonctionnement sont pris en charge par une plateforme unifiée de l'éducation nationale appelée CARIINA. Ce serveur, dans sa version complète (AMONECOLE) peut être le cœur d'une infrastructure informatique dans une école.

[13] URL : Uniform Ressource Location = adresse de la page internet

Fiche n° 10

LA FORMATION
DES DIFFÉRENTS
ACTEURS DU SI /
LA SENSIBILISATION
DES UTILISATEURS DU SI

Fiche n° 10

LA FORMATION DES DIFFÉRENTS ACTEURS DU SI / LA SENSIBILISATION DES UTILISATEURS DU SI

Synthèse

- Identifier les acteurs clés du système d'information pour les former
- Nommer un Responsable de la Sécurité des Systèmes d'Information (RSSI) quand le système devient complexe
- Mettre en place des sessions de formation pour les utilisateurs
- Sensibiliser à l'aide d'actions ponctuelles tous les acteurs du SI (administrateurs et utilisateurs)
- Bien mettre l'accent sur le côté professionnel de l'informatique de la collectivité

Nombre d'erreurs, qui sont commises dans l'implémentation d'une sécurité correcte, sont issues d'un manque de sensibilisation et de formation des acteurs des systèmes d'information. Or ces dernières années, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a mis en œuvre une politique de formation ambitieuse à l'égard des différents organes de l'état dont font partie les collectivités territoriales. Cette politique permet de former gratuitement les acteurs du SI à beaucoup d'aspects de la sécurité informatique.

Cette démarche n'est pas dénuée d'arrière-pensées puisque, plus les acteurs seront formés de manière correcte, moins les failles de sécurité seront béantes dans les collectivités et autres organismes d'état. Donc potentiellement, cette démarche s'inscrit dans la sécurisation accrue des données publiques. Le constat actuel dans la plupart des collectivités territoriales reste très contrasté en termes de maturité des systèmes d'information et donc par rebond, de leur sécurité globale.

La prise en compte de la sécurité des données doit être assumée au plus haut niveau de la hiérarchie. Si les responsables ne sont pas persuadés du bien-fondé de la chose, les propositions de sécurisation resteront lettre morte et l'absence d'évolution vers un système plus sécurisé sera fortement pénalisante pour l'ensemble des acteurs en cas d'attaque de quelque nature que ce soit. Dans les grandes structures, la nomination d'un RSSI peut être un atout majeur.

Cette personne est en effet dissociée de la DSI et ne rend des comptes généralement qu'au directeur général ou au Maire/Président. Cette « neutralité » fait du RSSI un observateur objectif du système puisqu'il n'en est pas partie prenante.

En ce qui concerne la sensibilisation des acteurs, ceux qui sont le moins formés dans la majeure partie des cas sont les utilisateurs finaux. Ce maillon de la chaîne reste le destinataire du SI mais n'en connaît généralement ni les tenants ni les aboutissants. Les erreurs commises le sont rarement volontairement, elles résultent plus souvent de la méconnaissance des menaces pesant sur le système d'information.

Pourquoi ne pas ouvrir une pièce jointe qui m'est destinée ? Pourquoi ne pas cliquer sur les liens qui sont contenus dans les mails ? Telles sont les questions que beaucoup d'utilisateurs se posent. Il ne suffit pas de « plaquer » des informations de sécurité. Si elles ne sont pas accompagnées d'un minimum, en termes d'explications supplémentaires, les consignes ne seront pas appliquées longtemps, car au final non comprises. Souvent, une demi-journée d'explication peut empêcher un certain nombre de « clics malheureux ».

Tout comme les utilisateurs finaux, les décideurs doivent être sensibilisés sur le sujet. En effet, au niveau des décisions et de l'organisation globale de la sécurité du système d'information, ils sont très sollicités. Or, si ces acteurs ne sont ni sensibilisés, ni formés aux rudiments de la sécurité informatique, ils ne seront pas à même de prendre les décisions qui s'imposent pour mettre le système dans des conditions de sécurité acceptables.

Enfin, il est très important de faire passer un message essentiel pour le bon déroulement d'une activité informatique professionnelle « nous ne sommes pas à la maison ». Cette phrase revient souvent dans la bouche des utilisateurs. Ils ont beaucoup de difficultés à faire le distinguo entre une informatique personnelle et une organisation informatique professionnelle. Les objectifs ne sont pas les mêmes et beaucoup ont du mal à le comprendre. Cet état de fait crée une vraie forme de danger car elle s'accompagne souvent de comportements à risque tels que les téléchargements sauvages, les utilisations de clés USB, la tentative d'aller sur des sites non autorisés… Dans tous les cas, la charte informatique peut « cadrer » l'utilisation de l'informatique et en préciser l'orientation strictement professionnelle.

Fiche n° 11

LES ORGANES DE LA SÉCURITÉ

Fiche n° 11
LES ORGANES DE LA SÉCURITÉ

Bien que l'aspect organisationnel dans la gestion de notre sécurité au quotidien soit adopté, la protection de notre information a besoin de s'appuyer sur des outils techniques qui vont nous permettre de répondre aux grands enjeux de la sécurité qui sont, la disponibilité, l'intégrité et la confidentialité.

Dans cette fiche, il sera abordé la définition des enjeux de sécurité, ainsi que des dispositifs de protection que l'on peut trouver entre le poste utilisateur et l'internet.

1. *Les enjeux de la sécurité*

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Celles-ci caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

- Disponibilité : demande que l'information sur le système soit disponible aux personnes autorisées et au bon moment.
- Confidentialité : demande que l'information sur le système ne puisse être accédée que par les personnes autorisées.
- Intégrité : demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées et habilitées.

Pour les organes nécessaires à la protection, il en existe 2 types :

- Des solutions couvrant la sécurité des accès,
- Des solutions couvrant la sécurité des contenus.

2. Postes de travail

Quand on évoque la sécurité d'un poste de travail, il vient naturellement à l'esprit « antivirus », outil indispensable qui ne couvre aujourd'hui qu'environ 45 % des menaces. Ci-après, sont présentés les organes à mettre en place pour protéger plus efficacement son poste.

L'antivirus

Ce dispositif repose principalement sur des bases de signature, sortes de vaccins pour ne pas laisser s'installer une maladie connue. Les virus étant apparus, il y a bien longtemps, les bases de signature sont colossales. De fait, il est fréquent de trouver des antivirus qui ne contiennent que des bases récentes, ce qui permet aux personnes mal attentionnées d'utiliser de vieux virus et ainsi passer cette barrière de protection pourtant à jour.

L'antimalware

Le malware est un type de virus doté d'une intelligence ne visant pas seulement la corruption de l'ordinateur mais également la prise de contrôle de ce dernier. Il cherche en conséquence à s'installer sur la machine, à y résider longtemps et si possible, se propager aux ordinateurs voisins ou distants.

Parmi les plus connus :

- Les vers : virus capables de se propager au travers du réseau,
- Les chevaux de troie (ou troyens) : virus qui permettent de créer une faille dans le système pour s'y introduire et y résider,
- Les spywares : logiciels espions destinés à recueillir de l'information (frappes clavier, copies d'écrans…),
- Les cryptolockers : programmes qui chiffrent le contenu des disques locaux ou réseau. Ils sont souvent accompagnés d'une demande de rançon afin que le pirate vous fournisse la clé pour déchiffrer les disques. On les appelle aussi des ransonwares.

Il existe des solutions de protection contre ces menaces. Cela se matérialise aussi bien par des logiciels à implémenter sur les postes que des dispositifs à placer au niveau du réseau.

Le pare-feu (firewall) personnel

Il a pour objectif principal de contrôler l'accès au réseau des applications installées sur l'ordinateur. Il permet de contrôler des programmes nuisibles (comme les chevaux de troie) ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un individu (ou un robot) à des fins malveillantes.

Ce dispositif est efficace mais nécessite des compétences pour sa gestion, notamment au niveau de la mise en place et du suivi des règles d'accès.

Le contrôle des périphériques

Le blocage des périphériques (clés USB, cartes mémoires, smartphone…) est aussi une mesure importante dans la protection du poste de travail. Les logiciels pour en assurer la gestion sont préconisés car ils permettent de ne pas tout interdire et de laisser un accès aux périphériques autorisés.
Un grand nombre de menaces étant véhiculées par ce biais, il est important de prendre cette mesure en considération même si parfois elle fait grincer des dents les utilisateurs.

Le chiffrement

Principalement utilisées sur les ordinateurs portables et les postes VIP, les solutions de chiffrement empêchent la lecture des données présentes sur le disque si la personne souhaitant y accéder ne possède pas la clé de déchiffrement. Cette solution était initialement lourde à mettre en œuvre. On la trouve aujourd'hui de façon native dans les systèmes Windows (à partir de Windows 7 Enterprise) via l'application « Bitlocker » et sur les machines elles-mêmes qui embarquent des puces Trusted Platform Module (TPM) qui est un composant matériel installé sur de nombreux ordinateurs récents.

BitLocker fournit donc une protection supplémentaire lorsqu'il est utilisé avec cette puce.

En conclusion, il est vrai que toute cette liste de composants peut s'avérer inquiétante. Mais depuis quelques années, les fournisseurs d'antivirus se sont orientés vers des solutions complètes que l'on trouve souvent sous le nom « Endpoint Security ». Elles comprennent une suite de logiciels permettant de réduire considérablement la surface d'exposition aux menaces.

Il est bon de rappeler aussi que les menaces exploitent des failles et que souvent les brèches sont béantes. Il faut alors adopter une bonne hygiène en limitant les droits d'accès aux postes (notamment les droits administrateurs), en verrouillant sa session lorsqu'on n'est pas devant son poste, en passant régulièrement les mises à jour (Windows, Adobe, Java…), et surtout en mettant un mot de passe renforcé qui ne doit être stocké que dans votre mémoire.

3. *Le réseau*

On parle souvent de la sécurité à la frontière du réseau et d'internet. En conséquence, la sécurité du réseau interne (LAN ou Intranet) est souvent négligée.

Les organes principaux des réseaux internes sont composés de commutateurs (souvent appelés switch) sur lesquels sont raccordés chacun des composants du système d'information (PC, copieurs, imprimantes, serveurs…). Il est dès lors très important d'y implémenter de la sécurité afin que ni personne, ni un équipement ne puisse s'y connecter sans avoir une autorisation. On peut implémenter des restrictions d'accès par « mac adress » qui est un identifiant matériel unique, ou bien par des protocoles d'authentification de type 802.1q. Il est important aussi de segmenter son réseau en zones (VLAN) et de contrôler les accès entre ces zones. Cette segmentation augmente la sécurité du réseau mais aussi ses performances.

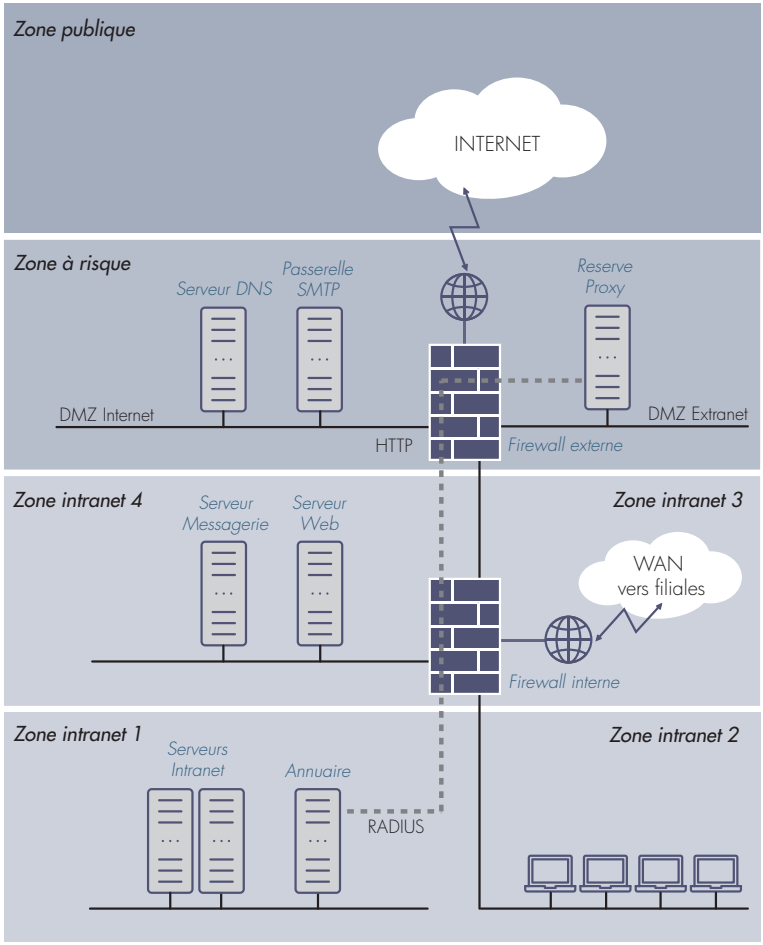
3.1. *Sécurité Internet (frontière réseau interne et réseau public)*

3.1.1. Les systèmes de pare-feu (Firewall)

C'est un système permettant de protéger le réseau interne contre les intrusions provenant d'un réseau tiers (notamment Internet). Il filtre les paquets de données échangés entre ces 2 réseaux. Il agit comme une passerelle filtrante, dans laquelle on enregistre des règles basées sur des autorisations (ou des noms autorisés) de communications entre différentes adresses (IP) via certains canaux que l'on appelle des ports comme http par exemple. Les firewalls ont évolué ces 10 dernières années vers des versions plus intelligentes visant à embarquer des fonctions supplémentaires de sécurité comme les UTM (Antivirus de flux, Proxy, Antimalware…) ou encore à appliquer des règles au niveau des utilisateurs et des applications, les « Nexgen Firewall »).

Beaucoup de flux traversent ces firewall. Aussi, afin d'accroître la protection du réseau interne, on crée sur ces pare-feu des zones démilitarisées (DMZ), que l'on utilise lorsque des machines précises du réseau doivent êtres accédées depuis l'extérieur, comme les serveurs de messagerie ou les serveurs Web. Cette zone accessible va alors servir de zone tampon dans laquelle seront analysés les flux. S'ils sont légitimes, alors seuls les firewalls seront habilités à envoyer l'information au serveur destinataire (comme par exemple le serveur de messagerie.)

Exemple d'une architecture sécurisée



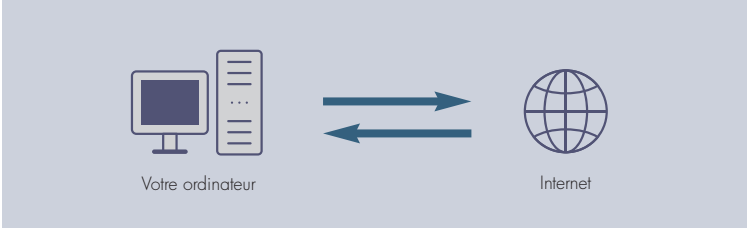
3.1.2. Les serveurs mandataires et mandataires inverses (Proxy et Reverses Proxy)

Ce sont des machines faisant fonction d'intermédiaire entre votre poste situé sur le réseau et internet. Ils sont principalement utilisés pour la navigation internet. On parle alors de proxy web ou proxy http.

Analogie

Imaginons que vous souhaitez acheter du pain, mais que vous ne voulez pas vous rendre à la boulangerie. Vous envoyez alors votre enfant remplir cette tâche. Il devient votre mandataire. Cependant, il va falloir qu'il paye pour vous, donc vous devrez lui fournir des informations confidentielles (code CB...), ce qui implique que vous ayez une grande confiance en lui pour que non seulement il remplisse sa tâche mais aussi, qu'il ne vide pas la boulangerie en achetant un kilo de bonbons. Votre enfant a en quelque sorte joué le rôle de proxy.

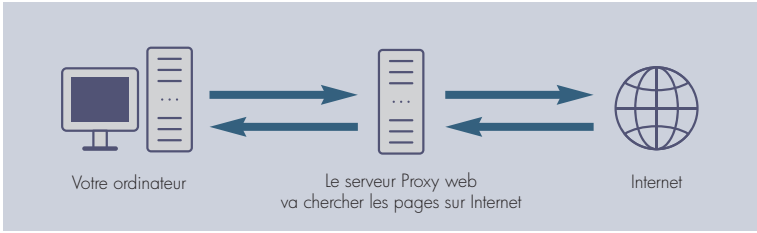
Lorsque vous surfez sur Internet, votre ordinateur est directement connecté. C'est lui qui va chercher les pages comme dans le schéma ci-dessous :



L'inconvénient principal de ce fonctionnement est que votre ordinateur est directement exposé sur Internet.

Si maintenant, on place un serveur proxy entre votre ordinateur et Internet, on obtient le schéma suivant :

→ votre ordinateur est connecté au serveur proxy,
→ et c'est lui qui est connecté à Internet.
→ vous demandez des pages à ce serveur,
→ il va chercher les pages demandées sur Internet
→ et vous renvoie les pages demandées.



Principaux avantages du Proxy

- **Le surf anonyme :** ce n'est pas votre adresse qui est vue sur les sites, mais l'adresse du proxy. Vous êtes ainsi « quasiment anonyme » ou « complètement anonyme » (voir un peu plus bas).

- **La protection de votre ordinateur :** ce n'est pas vous qui êtes en première ligne sur Internet, vous êtes donc mieux protégé.

- **Le masquage de votre lieu de connexion :** le proxy peut être dans un pays différent du vôtre. Lorsqu'il se connecte à un site, c'est la géolocalisation du proxy qui est vue, pas la vôtre. Cela peut être utile sur certains sites qui filtrent les connexions suivant les lieux d'où elles proviennent.

- **Le filtrage :** comme toutes les requêtes et les réponses passent par le proxy, il est possible de filtrer ce que l'on autorise à sortir ou à entrer. C'est le cas dans de nombreuses entreprises (nous y reviendrons plus loin).

Principaux inconvénients du Proxy

Qui dit avantages, dit également inconvénients. Comme nous l'avons vu au-dessus, c'est lui qui fait l'intermédiaire entre vous et le web. Donc il voit et peut enregistrer tout ce qui circule entre votre ordinateur et le web, et cela peut être risqué ! Imaginez juste que la personne qui gère ce serveur soit mal intentionnée. Elle a accès à l'ensemble de votre historique de navigation.

Il faut donc utiliser un proxy dont vous êtes sûr, ou alors ne pas l'utiliser : c'est-à-dire mettre des exceptions à l'utilisation de celui-ci. Sur certains sites, certains préconisent absolument d'utiliser des proxys pour être cachés, mais oublient de parler de la sécurité des données confidentielles que vous envoyez sur Internet.

Sachez cependant que vous avez une obligation de conserver les traces de connexion, et que vous devrez les fournir en cas de commission rogatoire. La mise en place de ce type d'équipement nécessite aussi une déclaration à la CNIL.

Si le serveur proxy est très sollicité, il peut éventuellement mettre plus longtemps à répondre. Donc, il est possible que le surf à travers un proxy soit un peu plus lent que le surf direct sur Internet.

Le reverse Proxy quant à lui fonctionne dans l'autre sens. Il joue le rôle d'intermédiaire entre l'internaute et une ressource que vous mettriez à sa disposition comme un site internet par exemple (portail citoyen, accès portail famille…)

Analogie

Situons-nous dans un café. Si vous souhaitez une boisson, vous n'allez pas aller directement vous servir derrière le bar, vous allez demander au garçon de café de vous apporter ce que vous désirez, et c'est ce dernier qui aura accès à la zone protégée où se trouvent les boissons et la caisse. Il agira donc en mandataire inverse (ou reverse proxy).

3.1.3. Les IDS/IPS (Intrusion Detection/Protection System)

C'est un organe basé sur un mécanisme écoutant le trafic réseau de manière furtive (non détectable) afin de repérer des activités anormales ou suspectes et permettant d'avoir une action de prévention sur les risques d'intrusion. Il fonctionne avec des bases de signatures mais aussi sur des analyses comportementales.

Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Ces équipements sont assez controversés car ils ont la réputation d'être très difficiles à régler (éviter les fausses alertes) et à gérer.

3.1.4. Antispam

Idéalement placé sur une zone démilitarisée, il fonctionne comme un proxy visant à protéger la messagerie de la collectivité contre les spam (pourriels) et les virus. Certaines solutions sont aussi embarquées sur les logiciels de messagerie eux-mêmes.

La technologie anti-spam moderne couvre un large éventail de filtres, de scanners et d'autres types d'applications. Certains services anti-spam fonctionnent à partir d'une méthode statistique (signatures), tandis que d'autres utilisent des méthodes heuristiques ou des algorithmes prédictifs. Pour trier le courrier de manière sophistiquée, les fournisseurs de service anti-spam peuvent surveiller les signatures électroniques, les adresses IP (blacklist de spammer) ou autres données, ce qui réduit le spam ; idéalement à placer sur le relais SMTP en DMZ, pour une plus grande efficacité.

Conclusion

Dans cette fiche, ont été décrits les organes principaux liés à la sécurité, mais il en existe bien d'autres (WAF, SandBox…) répondant à des menaces plus précises. Autant d'organes qu'il faudra maintenir à jour pour conserver leur efficacité.

Ces dispositifs sont techniques, mais une bonne partie de la sécurité repose sur une bonne appréciation des risques et une bonne hygiène informatique. Vous pourrez trouver bon nombre de mesures organisationnelles dans le guide d'hygiène informatique publié par l'ANSSI.

http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf

Sources : Blog Orange, ANSSI, Technopedia, culture informatique

Fiche n° 12

E-RÉPUTATION

Fiche n° 12
E-RÉPUTATION

Le concept d'« e-réputation », d'« identité numérique » ou encore d' « identité en ligne » fait son apparition dès le début des années 2000. Au départ, la réputation et l'e-réputation sont confondues, mais très vite l'e-réputation s'est différenciée pour plusieurs raisons comme la rapidité des communications, les volumes d'informations ou encore les personnes cibles.

La réputation touchait classiquement une collectivité ou une entreprise, c'est-à-dire une personne morale. Aujourd'hui, l'e-réputation est complétement rattachable à une personne physique, ce qui peut engendrer de lourdes conséquences lorsqu'il s'agit d'élus ou de personnes publiques.

Aujourd'hui, on assiste alors au mouvement inverse, l'identité numérique se confondant de plus en plus dans la réputation dite « classique », tant son influence devient importante, que ce soit en bien ou en mal.

Nous ferons donc un tour d'horizon de « l'e-réputation » en précisant sa définition mais en abordant aussi les façons de la développer ou de se protéger contre plusieurs formes d'attaques visant à impacter la réputation numérique des personnes morales, ou des personnes physiques.

1. *Définitions*

L'e-réputation est la réputation, l'opinion commune (informations, avis, échanges, commentaires, rumeurs…) sur les réseaux d'une entité (marque, personne morale) ou physique (particulier, personne publique), réelle (représentée par un nom ou un pseudonyme) ou fictive. Elle correspond à l'identité de cette marque ou de cette personne associée à la perception que les internautes s'en font.

L'e-réputation est créée par :

→ ce que l'organisation ou la personne dit sur elle explicitement :
- actions de communication, communiqués de presse, interviews des dirigeants, cadres

→ ce qu'elle dit sur elle implicitement :
- actes qui peuvent être traçables
  exemple : modification de contenu sur wikipédia

→ ce que ses employés disent d'elle explicitement, généralement de manière anonyme :
- exemple : sites pour noter son entreprise, commentaire sur les réseaux sociaux

→ ce que ses employés disent d'elle implicitement :
- exemple : données professionnelles mises en ligne sur LinkedIn ou Viadeo (fonction, sujet de travail) qui, une fois agrégées, peuvent fournir d'intéressantes informations

→ ce que ses clients disent d'elle explicitement :
- exemple : blogs d'utilisateurs d'un produit, forums de discussion

→ ce qu'ils en disent implicitement :
- systèmes de notation d'entreprise / de collectivité

→ ce que ses concurrents disent d'elle explicitement :
- publicités comparatives

→ ce qu'ils disent de manière anonyme :
- attaque dans des forums de discussion, création de vrais-faux blogs et tout ce qui s'apparente à des actions de déstabilisation par l'information

→ ce que des personnes-relais qui ne sont aucune des entités déjà identifiées en disent :
- bloggeurs qui relaient une info
- utilisateurs de réseaux sociaux

Ce sont donc autant d'éléments que doit être à même d'apprécier et de surveiller une collectivité et / ou une personne physique afin de veiller à l'évolution de sa réputation virtuelle.

1.1. *Rappel des risques de la publication sur internet*

Toutes les données publiées sur internet sont publiques. Dès lors, avant toute communication, il faut vérifier son utilité, sa formulation, son impact potentiel, ses cibles, et si possible ses faiblesses. En effet, la rapidité de propagation qu'est le vecteur internet empêche toute suppression ou modification ultérieure du message. Il y aura toujours quelqu'un pour vous rappeler à vos erreurs si des modifications ou des changements devaient être effectués sur une communication maladroite, inefficace ou franchement ratée.

Du reste, il n'existe pas de communication « parfaite », tous les détails et facteurs ne pouvant être pris en compte. Il faut donc être à même de pouvoir répondre à ses détracteurs avant que la situation ne s'envenime.

Dans le cadre d'une personne physique, les publications sur internet sont généralement l'expression de sentiments, de considérations, de réflexions… Il faut garder à l'esprit que ces déclarations représentent une opinion, un point de vue sur une situation, et cela vous engage. Il est évident que tous ne partageront pas votre opinion, et donc là encore, il faut se préparer à protéger son identité numérique.

De plus, il faut toujours garder en mémoire que les images publiées sur des réseaux sociaux ne sont plus la propriété de la personne qui les a mises en ligne, ce qui rendra d'autant plus difficiles les possibilités de récupération ou d'effacement.

Certains mettront en avant le droit à l'oubli. Pourtant, ce droit est souvent mal apprécié : les cas qu'il recouvre sont restreints et limités. Ainsi, le droit à l'oubli permet à tout internaute européen qui en fait la demande, d'obtenir le déférencement de contenus de nature à porter atteinte au respect de la vie privée. En conséquence, il ne peut s'appliquer aux contenus postés par la personne physique dans le cadre des réseaux sociaux, par exemple.

2. *Les profils qui menacent l'e-réputation*

On peut ranger ces profils suivant 4 catégories : les amères, les rancuniers, les détracteurs et enfin les « trolls ».

Les détracteurs

Ils s'estiment au-dessus des autres. Ils sont moralistes-politico-économistes, croient avoir la science infuse et savent expliquer aux autres combien leur vision est juste et avisée. Sous des airs de bienveillance (ils veulent toujours paraître utiles aux autres en dénonçant des faits), ils font d'un débat un combat personnel, rempli par leur conviction : prévenir les autres d'un grand danger. Cela pourrait être louable s'il n'y avait pas de propos dénigrants ou diffamatoires. Ils peuvent fédérer bien plus que les amères et les rancuniers, car ils reposent leurs actions sur des idéologies souvent propices à des réactions formulées par leurs semblables. Des débats sans fin qui s'imprègnent profondément dans les méandres des moteurs de recherche.

Les amères

L'amertume est un mélange de colère, de révolte et de tristesse à l'égard de souffrances que l'on a vécues comme étant injustes. Heureusement, la notion de tristesse dévoile une certaine humanité encore présente et peut-être donc préserver quelques valeurs morales dans ce désert d'incompréhension et de frustration. Les amères ont un besoin intrinsèque d'exprimer leur version des choses. Ils ne vont donc pas s'en priver et déballer clairement tout le dossier en détail, pièces jointes à l'appui, car ce sont des procéduriers en général et de fins investigateurs. Une fois libérés, ils s'apaisent généralement tous seuls, comme une bougie, ils s'éteignent lentement, mais leur cire reste longtemps collée à la toile.

Les rancuniers

La rancune est une colère qui contient un désir de vengeance. Ils ont été frustrés par une situation, ils se sont sentis humiliés ou tout simplement inférieurs face à une personne ou tout un groupe. Ils vont alors mettre en place toute une campagne malveillante en crachant leur venin partout où il pourra être viral : cela commence par leur propre Blog, leur Facebook, Twitter et autres réseaux sociaux. Ils assument complètement leurs propos en affichant leur identité. Tenter de concilier avec eux est vain. Tenter des recours juridiques peut finir à la longue par les calmer, mais avant cela, ils se montreront encore plus virulents face à une riposte. Enfermés dans leur vérité et leurs ressentiments, ils n'auront d'autre but dans leur vie, du matin au soir et du soir au matin, que de se venger et nuire à leur(s) ennemi(s). Ils sont à traiter avec subtilité et délicatesse et surtout pas de front, car certains ne craignent ni la justice ni la loi du Talion.

Les « trolls »

Véritable fléau de l'internet, le « troll » est là pour vous dénigrer quoiqu'il arrive. Il usera de tous les moyens pour vous faire franchir la ligne blanche, celle du non-retour, dans le but de vous accabler encore plus. Aucun débat n'est possible tant il usera de mauvaise foi, d'arguments fallacieux et de détournement de vos propos pour servir sa cause. Dans le cadre des personnes physiques le « troll » fera son possible pour pousser son interlocuteur à la faute (propos injurieux, diffamatoire, ou tout simplement faux).

2.1. *Quelles attitudes adopter ?*

Quelle attitude avoir face à ces profils ? Evidemment, il ne peut y avoir de réponse générique, tant la diversité des situations est grande. Néanmoins, quelques grands traits caractéristiques peuvent être explicités :

Conserver son sang-froid

Facile à dire quand un nom est sali, mais essentiel à faire avant toute riposte qui pourrait être influencée par un sentiment tout aussi mauvais que celui qu'on découvre.

Creuser sur internet

Pour découvrir d'éventuels autres liens défavorables, puis les répertorier. Enfin, il faudra étudier leur contenu et leur sens, leur potentiel de viralité, les éventuels engagements obtenus par d'autres internautes qui viendraient prendre part à la discussion (les identifier si possible), ainsi que leur positionnement sur les moteurs de recherche. Cela s'appelle faire un audit.

Mettre en place une stratégie de défense rapide

Une réponse adaptée aux profils doit être mise en place. Elle peut être de l'ordre d'un simple échange argumentaire au sein d'un fil de discussions sur un blog, un forum ou un réseau social.

Cela peut être la mise en place immédiate d'une notoriété positive et de la création de contenu à la fois pertinent et volumineux.

Cela peut être enfin une démarche plus stratégique à long terme dès lors qu'il s'agit d'amères ou de rancuniers.

Dans tous les cas, il faut réagir dans le calme avec fermeté, patience, stratégie et bienveillance.

Bienveillance, à travers tous les propos que vous vous apprêtez à publier. On doit sentir que vous êtes sain, honnête et surtout pas comme eux.

Le rassemblement d'une armée « d'ambassadeurs » et de « recommandeurs » doit aussi être envisagé pour donner du crédit à votre image et contribuer à rendre irrecevables les propos diffamatoires, suspicions gratuites et autres insultes à votre personne.

Enfin parfois, la solution juridique doit être envisagée : les propos diffamatoires ou injurieux, le dénigrement et les atteintes aux droits de la personne sont répréhensibles juridiquement. Ces recours doivent être maniés avec parcimonie. En effet, votre action, bien que fondée, pourra nuire grandement à votre réputation numérique.

Dans tous les cas, ne restez pas seul, ne prenez pas tout au premier degré, et dans la mesure du possible, gardez un certain sens de l'humour : il peut complétement retourner une situation défavorable en situation favorable pour votre e-réputation.

Enfin, si vous souhaitez avoir une présence sur Internet, entourez-vous de spécialistes nommés « community manager », formés pour veiller à votre image, votre réputation et répondre le plus efficacement possible aux problématiques concernant votre identité numérique.

3. *Quelques outils*

Il y a des agences spécialisées aussi bien dans la surveillance de votre e-réputation que dans les démarches vous accompagnant dans la suppression de vos données présentes sur internet.

Il existe aussi des outils (gratuits ou payants) qui vous permettent d'initier ces démarches. Vous en trouverez ci-dessous quelques-uns.

3.1. *Pour vérifier et surveiller sa présence sur internet*

Recherche Google : eh oui, une simple recherche sur votre nom, en image ou actualité vous donnera un bon aperçu de votre présence.

Google Alert, qui vous préviendra dès qu'un de vos critères de recherche (nom, entreprise,…) sera référencé.

Mais aussi (gratuits), mention.net, fr.alerti.com, Hootsuite, owler, trackur…

3.2. *Pour effacer ses données*

L'idéal est de confier cette tâche à des acteurs spécialisés. Cependant, il existe des outils mis à votre disposition gratuitement pour vous aider à initier votre démarche. Citons des sites comme forget.me, justdelete.me.

Enfin, vous trouverez aussi beaucoup de ressources intéressantes sur le site de la mairie de Paris, à l'initiative du programme « soyez net sur le net » http://ereputation.paris.fr/.

Fiche n° 13

CONDUITE À TENIR EN CAS D'ATTAQUE

Fiche n° 13
CONDUITE À TENIR EN CAS D'ATTAQUE

Savoir agir lorsque l'administration est victime d'une cyberattaque est primordial pour limiter les risques et rétablir rapidement une situation normale. La procédure à suivre doit être définie et comprend des démarches techniques et des démarches administratives.

Pour que les actions à mener soient coordonnées et efficaces, le référent technique (DSI, ingénieur, technicien informatique…) et le référent administratif (élu, DGS, DGA, responsable administratif…) doivent avoir été désignés au préalable dans chaque administration.

Ces référents doivent être formés et sensibilisés aux problématiques liées à la cybercriminalité et aux procédures d'intervention. Ainsi, en cas d'attaque, aucune action ne peut être menée sans leur accord.

Une fois désignés, les référents définissent la procédure d'intervention et le rôle de chacun afin de pouvoir intervenir d'une manière efficace et efficiente.

Etape 1 : Identifier l'attaque

Quelle est la nature de l'attaque ? Qui est visé ? Quel est le moyen utilisé (clé USB, virus, téléchargement…) ? Les structures extérieures ou annexes sont-elles touchées ?

Rôle du référent technique qui en informe, immédiatement, le référent administratif.

Etape 2 (ou 3) : faire cesser l'attaque

L'ordinateur ou l'équipement potentiellement incriminé doit être déconnecté sans l'éteindre. L'intervenant doit veiller à la préservation des preuves.

Rôle du référent technique

Etape 3 (ou 2 selon la nature de l'attaque) : Faire constater l'attaque

La première constatation est réalisée par le référent technique.

Constater soi-même l'attaque ou par le biais du prestataire extérieur, le cas échéant.

Si l'attaque revêt une forme grave (vol de données, image des élus, attaque terroriste…), il y a lieu de la faire constater par un huissier ou les forces de l'ordre.

Le choix du mode de constatation relève de la compétence du référent administratif.

Etape 4 : Constituer les preuves

Pour être recevables, les preuves doivent être licites. Leur collecte doit se faire légalement (pour exemple : est considérée comme illicite une preuve qui serait obtenue par le piratage du compte de l'agresseur).

Les preuves peuvent être : des captures d'écran, des images du réseau, un journal de connexion…

Constituer les preuves rapidement après l'attaque est vital compte tenu du temps de conservation des données numériques. Aucune manipulation qui pourrait endommager les preuves ne doit être effectuée.

Rôle du référent technique

Etape 5 : Déposer plainte

Selon la gravité de l'attaque et des préjudices subis, il est possible de porter plainte auprès de l'enquêteur spécialisé en criminalité informatique de la Police Nationale (ESCI), de l'enquêteur spécialisé dans les nouvelles technologies de la Gendarmerie Nationale (NTECH) ou auprès du procureur de la République.

L'opportunité des poursuites appartient au procureur de la République en fonction notamment de la nature de l'attaque, des preuves constituées et de la conclusion de l'enquête judiciaire.

Rôle du référent administratif

Etape 5 : Restaurer le système

Compte tenu de la « dépendance » de la majorité des services à l'informatique, il convient de rétablir rapidement les outils nécessaires à la continuité du service public.

La restauration ne doit pas intervenir dans la précipitation. Les risques doivent être pris en compte et des solutions doivent être mises en place.

Rôle du référent technique

Etape 6 : Communiquer

Etablir un plan de communication en fonction de la nature de l'attaque (rétablir l'image des élus, communication sous forme de courrier aux habitants en cas de vol de données ou de piratage de dossiers les concernant, communication sur le site internet une fois rétabli, bulletin municipal, communication aux candidats à un marché public, communication aux comptables et services de l'Etat, communication nationale si acte terroriste…). La communication doit être proportionnelle à l'ampleur des préjudices.

Rôle du référent administratif

Etape 7 : Réparer les préjudices

Lorsque l'administration est assurée contre les cyber-risques, l'assureur doit être informé dès la survenance de l'attaque afin de déterminer les risques couverts et les sinistres pouvant être pris en charge (voir la fiche n° 14 « Les risques pouvant être couverts par une assurance »).

Rôle du référent administratif

La conduite à tenir dans le cadre d'une attaque en crypto malware :

- Isolation du poste incriminé par déconnexion du câble RJ45 et extinction de ce dernier.
- Alerte immédiate auprès du service en gestion de l'informatique (exploitation, DSI, RSSI).
- Recherche immédiate sur les serveurs par les équipes techniques de l'ensemble des fichiers chiffrés et considérés comme irrécupérables.
- Restauration des fichiers chiffrés et destruction de ces derniers (leur conservation ne sert à rien car la probabilité de voir arriver un outil de déchiffrement sûr dans des délais raisonnables est extrêmement faible).
- Formatage complet et remise à zéro du poste incriminé après récupération des données, restant non chiffrées et exploitables, sur le disque dur de la station incriminée à l'aide d'une station blanche (non reliée au réseau et dont la compromission potentielle n'affecterait en rien le fonctionnement du système d'information).

Fiche n° 14

LE RISQUE DE CYBERATTAQUE : COMMENT VOUS ASSURER ?

Fiche n° 14
LE RISQUE DE CYBERATTAQUE : COMMENT VOUS ASSURER ?

Quelques chiffres clés

Source : étude PWC 2014, « Global Economic Crime Survey »

Les cyber-risques représentent les atteintes aux systèmes d'informations ainsi que l'atteinte aux données numériques détenues et/ou gérées par la collectivité, que celles-ci lui appartiennent ou qu'elles lui soient confiées par des tiers. Les auteurs d'attaques sont de plus en plus ingénieux. Les cybercriminels tirent profit d'une surface d'attaque en pleine expansion en raison de l'hyper-dépendance à l'informatique (réseau, internet, wifi), la dématérialisation des données et du développement des nouvelles technologies (mobilité, cloud-computing, data center, externalisation de services informatiques…).

Le contexte actuel n'est pas favorable. En effet, suite aux attentats de Charlie Hebdo, une vague de cyberattaques a ciblé des milliers de collectivités (Le mémorial de Caen, la Communauté de Communes de Charente les 4B, l'office de tourisme de Biarritz…).

Vous êtes concerné, quelle que soit la taille de votre collectivité. Le danger réside tant dans la sécurité mise en place par le DSI que dans le comportement d'un agent exposé à une cyberattaque.

Quelques exemples de cyberattaques

La Mairie de Fontenay-le-Comte victime d'une cyber extorsion

Un blocage de 68 000 dossiers informatiques par un hacker a paralysé tout le système informatique de la collectivité.

La prise d'otages et le cryptage des données personnelles (fiches de paie, analyses techniques, délibérations, etc.) se sont déroulés en une fraction de seconde.

Ouest-France – 21/01/15

La Mairie de La-Roche-sur-Foron victime d'un acte de Phishing

Un seul petit clic pour ouvrir une pièce jointe, et tous les comptes informatiques de la Mairie de La-Roche-sur-Foron ont été contaminés.

Un agent a reçu un e-mail avec, en pièce jointe, une facture d'une entreprise connue des services de la Mairie. Par automatisme et inadvertance, l'agent a ouvert le document sans s'apercevoir qu'il s'agissait d'un piège.

Ce n'est qu'en fin d'après-midi que les services de la Mairie ont constaté que tous les ordinateurs avaient été contaminés par un virus.

Le Dauphiné – 08/02/15

LA QUESTION N'EST PAS DE SAVOIR SI VOUS ALLEZ VOUS FAIRE PIRATER… MAIS QUAND ?

Le contrat d'assurance cyber : une solution complète de prise en charge des conséquences financières d'une cyberattaque

ÉVÉNEMENTS GARANTIS :
Atteintes aux données numériques et / ou aux systèmes d'information

3 VOLETS DE GARANTIES

DOMMAGES	ASSISTANCE ET GESTION DE CRISE	RC
Vol, détérioration, destruction de données, impossibilité d'utiliser les systèmes, contamination.		Atteinte à la vie privée, diffamation, divulgation d'informations confidentielles, atteinte au droit de la propriété intellectuelle.
CYBER EXTORSION : • Frais des consultants, • Remboursement de la rançon.	• Frais de notification aux personnes et à l'autorité compétente, • Frais de monitoring, expert en sécurité informatique, • Frais de gestion de crise, services (prestations de coaching, frais d'avocat, prestataires informatiques…), • Frais de communication, préservation de l'image de la collectivité, • Enquête et sanction d'une autorité administrative.	FRAIS ET CONSÉQUENCES PÉCUNIAIRES : • Frais de défense et conséquences pécuniaires suite à réclamation de tiers, • Sanctions pécuniaires, • Dommages et intérêts.

Un accompagnement ingénierie personnalisé

En complément d'une assurance cyber, un accompagnement en prévention des cyber-risques personnalisé peut être mis en place pour aider votre collectivité à faire face aux nouveaux risques et à la malveillance informatique.

En s'appuyant sur les moyens de prévention et de protection déjà opérationnels dans votre collectivité, l'accompagnement ingénierie vise à réduire la vulnérabilité de vos systèmes d'information ainsi que les conséquences des éventuelles cyberattaques.

Ce service comporte :

- Un audit préalable donnant lieu à la remise d'un diagnostic sur-mesure complété par des conseils personnalisés,

- Un accompagnement dans la durée en ingénierie cyber.

Fiche n° 15

MISE EN PLACE
D'UNE POLITIQUE
DE SÉCURITÉ DES SYSTÈMES
D'INFORMATION (PSSI)

Fiche n° 15

MISE EN PLACE D'UNE POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI)

Définition d'une PSSI :

La PSSI constitue le principal document de référence en matière de SSI. Elle en est un élément fondateur, au même titre qu'un schéma directeur, qui lui, définit les objectifs à atteindre et les moyens accordés pour y parvenir. Ces documents sont établis en fonction de la culture et du référentiel déjà existant dans la collectivité.

Ce document doit être décidé et appuyé au plus haut niveau de la hiérarchie car il est constitutif de la future sécurité du système d'information. Il doit être bien cadré afin de définir les axes stratégiques de la mise en place des futures procédures. Les enjeux, les choix et la prise en compte du risque sont déterminés durant cette phase initiale.

Le concept de la démarche d'élaboration d'une PSSI se déroule en 4 phases successives :

- Phase 0 : préalables
    - Tâche 1 : organisation projet
    - Tâche 2 : constitution du référentiel

- Phase 1 : élaboration des éléments stratégiques
    - Tâche 1 : définition du périmètre de la PSSI
    - Tâche 2 : détermination des enjeux et orientations stratégiques
    - Tâche 3 : prise en compte des aspects légaux et réglementaires
    - Tâche 4 : élaboration d'une échelle de besoins
    - Tâche 5 : expression des besoins de sécurité
    - Tâche 6 : identification des origines des menaces

- Phase 2 : sélection des principes et rédaction des règles
    - Tâche 1 : choix des principes de sécurité
    - Tâche 2 : élaboration des règles de sécurité
    - Tâche 3 : élaboration des notes de synthèse

- Phase 3 : finalisation
    - Tâche 1 : finalisation et validation de la PSSI
    - Tâche 2 : élaboration et validation du plan d'action

Les suites à donner à l'élaboration d'une PSSI s'articulent autour de quatre axes fondamentaux :

1. Assurer une déclinaison opérationnelle des règles de la PSSI, notamment sous la forme de procédures, applicables directement aux différents systèmes et applications.

2. Constituer une entité de suivi et de pilotage du plan d'action prioritaire défini à l'issue de cette démarche. La vision dynamique, nécessaire pour prendre en compte la sécurité dans un contexte mouvant, peut conduire à remettre en question des priorités du plan d'action et donc à réitérer au moins la fin de la démarche.

3. L'audit de la PSSI, notamment construit autour de contrôles réguliers à plusieurs niveaux de l'application opérationnelle ou à l'aide de tableaux de bord SSI, est un élément fondamental pour assurer l'efficacité de la couverture des risques jugés inacceptables. Ainsi, les résultats obtenus à l'issue de ces audits (organisationnels et techniques) pourront, le cas échéant, demander une révision des règles de sécurité.

4. Enfin, la mise en place d'une organisation d'alerte et de veille technologique est nécessaire à assurer la maintenance du niveau de sécurité et son efficacité dans le temps.

Fiche n° 16

LE PLAN REPRISE D'ACTIVITÉ (PRA) / LE PLAN CONTINUITÉ D'ACTIVITÉ (PCA)

Fiche n° 16

LE PLAN REPRISE D'ACTIVITÉ (PRA) / LE PLAN CONTINUITÉ D'ACTIVITÉ (PCA)

Préambule

L'incident de sécurité majeur et impactant lourdement le système d'information est, de nos jours et ce malgré l'ensemble des solutions de sécurité existantes, quasiment inévitable. Il est donc nécessaire de prévoir cet incident et surtout de mettre en place des mécanismes pour pallier les dégâts infligés à l'infrastructure. Un des moyens les plus sûrs est de se doter de procédures de reprise d'activité et de restauration de données. Ces différents éléments sont à mettre en place en fonction du besoin exprimé par la collectivité sur les éléments fonctionnels critiques du système préalablement identifiés.

Un Plan de Reprise d'Activité permet d'assurer, en cas de crise majeure ou importante d'un système informatique, la reconstruction de son infrastructure et la remise en route des applications vitales au fonctionnement d'une entité.

Le Plan de Reprise d'Activité doit permettre, en cas de sinistre, de basculer sur un système de substitution capable de prendre en charge les besoins informatiques nécessaires au fonctionnement minimal de la collectivité. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par les élus en charge de la question.

Le Plan de Reprise d'Activité (PRA) est à distinguer du Plan de Continuité d'Activité (PCA) : ce dernier a pour objectif de poursuivre l'activité du service sans interruption et d'assurer la disponibilité des informations quels que soient les problèmes rencontrés. Le PRA en est un sous-ensemble qui décrit les mesures qui doivent être déclenchées à la survenue d'un sinistre ou incident majeur ayant entraîné une interruption de l'activité.

Pour être efficace, ce plan de reprise doit être validé par les utilisateurs des différentes solutions et testé de manière régulière en fonction de l'évolution du système d'information. La mise en fonction de manière unique d'un plan lors d'une panne majeure d'un système est vouée à l'échec. Elle peut même, au pire, être contre-productive et faire perdre un temps précieux dans la remise en route des éléments de production.

Le Plan de Reprise parfait et standard n'existe pas. Chacune des collectivités mettant en place ce type de procédure devra le faire de manière unique. Cette procédure est, en effet, fortement liée à l'organisation de son entité et à son système d'information souvent propre à une collectivité et ce, quelle que soit sa taille.

Ces procédures dans leur ensemble sont très peu mises en place en collectivité de manière rigoureuse car très coûteuses et pas toujours pertinentes. La perte d'exploitation, si elle n'est pas trop importante, reste plus possible pour une administration que pour une société dont l'économie repose essentiellement sur son Système d'information.

Cependant, cette perte d'exploitation doit être minimisée au maximum pour éviter tout arrêt de l'activité préjudiciable en termes d'image et en termes financiers.

Etapes de la mise en place d'un plan de reprise / continuité

Pour qu'un plan de reprise/continuité soit réellement adapté aux exigences de la collectivité, il doit reposer sur une analyse de risque et une analyse d'impact :

L'analyse de risque débute par une identification des menaces sur l'informatique. Les menaces peuvent être d'origine humaine ou « naturelle ». Elles peuvent être internes à l'entreprise ou externes. On déduit ensuite le risque qui découle des menaces identifiées, on en mesure l'impact possible. Enfin, on décide de mettre en œuvre des mesures d'atténuation des risques en se concentrant sur ceux qui ont un impact significatif.

L'analyse d'impact consiste à évaluer quel est l'impact d'un risque qui se matérialise, et à déterminer à partir de quand cet impact est intolérable, généralement parce qu'il met en danger les processus essentiels de la collectivité.

Une analyse de risque réussie est le résultat d'une action collective impliquant tous les acteurs du système d'information : techniciens, utilisateurs et managers.

Choix de la stratégie de sécurisation

Il existe plusieurs méthodes pour assurer la continuité de service d'un système d'information.

Les méthodes se distinguent entre préventives et curatives. Les méthodes préventives sont souvent privilégiées, mais décrire les méthodes curatives est une nécessité car aucun système n'est fiable à 100 %.

Pour une mise en œuvre dans de bonnes conditions, il faut établir les procédures suivantes :

Les procédures qui mettent la stratégie en œuvre. Ceci inclut les procédures d'intervention immédiate (qui prévenir ? qui peut démarrer le plan et sur quels critères ? où les équipes doivent-elles se réunir ? etc.).

Les procédures pour rétablir les services essentiels, y compris le rôle des prestataires externes.

Toutes ces procédures doivent être accessibles aux membres des équipes de pilotage, même en cas d'indisponibilité des bâtiments.

Mesures préventives

La sauvegarde des données

Voir la fiche n° 3 page 25.

Les systèmes de secours

Il s'agit de disposer d'un système informatique équivalent à celui pour lequel on veut limiter l'indisponibilité : ordinateurs, périphériques, systèmes d'exploitation, programmes particuliers, etc. Une des solutions consiste à créer et maintenir un site de secours, contenant un système en ordre de marche capable de prendre le relais du système défaillant. Selon que le système de secours sera implanté sur le site d'exploitation ou sur un lieu géographiquement différent, on parlera d'un secours in situ ou d'un secours déporté.

Pour répondre aux problématiques de recouvrement de désastre, on utilise de plus en plus fréquemment des sites délocalisés. Ces solutions sont de plus en plus proposées par les éditeurs de logiciels métiers. Elles restent toutefois très dépendantes de la bande passante disponible sur la zone d'exploitation.

Les sites de secours (in situ ou déportés) se classent selon les types suivants :

- Salle blanche (une salle machine protégée par des procédures d'accès particulières, généralement secourue électriquement). Par extension, on parle de salle noire pour une salle blanche entièrement pilotée à distance, sans aucun opérateur à l'intérieur.

- Site chaud : site de secours où l'ensemble des serveurs et autres systèmes sont allumés, à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêts à fonctionner.

- Site froid : site de secours qui peut avoir une autre utilisation en temps normal. Les serveurs et autres systèmes sont stockés mais non installés, connectés, etc. Lors d'un sinistre, un important travail doit être effectué pour mettre en service le site, ce qui conduit à des temps de reprise longs (quelques jours). Mais son coût de fonctionnement, hors période d'activation, est faible, voire nul.

- Site tiède : site de secours intermédiaire. En général, on trouve des machines installées (mise à jour décalée par rapport au site de production) avec les données sur bande mais non importées dans les systèmes de données.

Plus les temps de rétablissement garantis sont courts, plus la stratégie est coûteuse. Il faut donc choisir la stratégie qui offre le meilleur équilibre entre le coût et la rapidité de reprise.

Mesures curatives

Selon la gravité du sinistre et la criticité du système en panne, les mesures de rétablissement seront différentes.

La reprise des données

Dans cette hypothèse, seules des données ont été perdues. L'utilisation des sauvegardes est nécessaire et la méthode, pour simplifier, consiste à réimplanter le dernier jeu de sauvegardes. Cela peut se faire dans un laps de temps court (quelques heures), si l'on a bien identifié les données à reprendre et si les méthodes et outils de réimplantation sont accessibles et connus.

Le redémarrage des applications

A un seuil de panne, plus important, une ou des applications sont indisponibles. L'utilisation d'un site de secours est envisageable, le temps de rendre disponible l'application en cause.

Le redémarrage des machines

- Provisoire : utilisation des sites de secours
- Définitif : après dépannage de la machine d'exploitation habituelle, y rebasculer les utilisateurs, en s'assurant de ne pas perdre de données et si possible de ne pas déconnecter les utilisateurs.

Exercices et maintenance

Le but de l'exercice est multiple :

- Vérifier que les procédures permettent d'assurer la reprise/continuité d'activité
- Vérifier que le plan est complet et réalisable
- Maintenir un niveau de compétence suffisant parmi les équipes de pilotage
- Évaluer la résistance au stress des équipes de pilotage

Un plan doit aussi être revu et mis à jour régulièrement (au moins une fois par an) pour tenir compte de l'évolution de la technologie et des objectifs de la collectivité.

Fiche n° 17

LA GESTION DES EMAILS

Fiche n° 17
LA GESTION DES EMAILS

Les courriers électroniques sont devenus les vecteurs principaux de communication dans le milieu professionnel. Cela implique diverses choses, le nombre des emails a explosé ces dernières années. Avec cette explosion, les emails frauduleux sont devenus monnaie courante (le phishing, les spams, les scams et autres mails avec des pièces jointes corrompues).

A l'heure actuelle, on estime que sur l'internet mondial, 3 millions de spams sont envoyés par seconde. Cela représente une charge de gestion non négligeable et un impact écologique énorme (33 Milliards de KWH par an et 17 Millions de tonnes de CO2 pour l'année 2009).

L'ensemble de ces mails est destiné à une seule et unique chose, piéger l'internaute qui cliquera sur le lien ou la pièce jointe.

Quelques règles de bonne conduite simples peuvent permettre d'éliminer une partie des risques liés aux emails.

Conseil n° 1

Ne jamais utiliser son adresse professionnelle à des fins d'inscription privée sur des sites internet. Ce conseil peut s'ériger en règle dans certaines collectivités en liaison avec leur charte d'utilisation des ressources des Techniques de l'Information et de la Communication (TIC).

Conseil n° 2

Ne jamais cliquer sur un lien ou ouvrir une pièce jointe d'un expéditeur inconnu. Cela paraît évident, mais dans la précipitation, il reste facile de commettre une erreur de ce type. Les spams sont de mieux en mieux conçus et certains peuvent être très proches des mails professionnels que l'on reçoit habituellement.

Dans tous les cas, sauf sur des cas bien identifiés, il est nécessaire de se poser la question de la validité avant l'ouverture de quelque mail que ce soit.

Conseil n° 3

Ne pas diffuser son adresse professionnelle sur les réseaux sociaux.

Conseil n° 4

Ne pas participer aux « chaînes de solidarité » en tout genre qui permettent de récupérer des adresses en grand nombre en bout de chaîne.

Conseil n° 5

Lors d'un transfert de mail, penser à effacer les adresses déjà présentes dans le mail et qui ne sont pas nécessaires à la compréhension du sens du message.

Conseil n° 6

Mettre les listes de diffusion en cci lors des envois massifs pour ne pas permettre la captation des adresses de ces listes.

Ces quelques conseils ne sont pas exhaustifs et la vigilance doit être la plus importante possible dans la manipulation de cet outil qui est devenu indispensable mais aussi source de problèmes multiples. Là encore, la sensibilisation et la formation des personnels exécutants peut être un plus pour une meilleure compréhension de la menace liée à la messagerie électronique.

Fiche n° 18

LES NORMES RÉGISSANT LES SYSTÈMES D'INFORMATION DANS LEUR ENSEMBLE

Fiche n° 18
LES NORMES RÉGISSANT LES SYSTÈMES D'INFORMATION DANS LEUR ENSEMBLE

Liste de normes internationales reconnues de gouvernance, d'audit, de sécurité et de qualité informatique, des systèmes d'information

Le référentiel CobiT

Référentiel de gouvernance et d'audit informatique.

Normes ISO 20000

Les normes ISO 20000-1 et ISO 20000-2 sont des standards décrivant des processus de gestion pour la livraison efficace et efficiente de services informatiques à l'entreprise et à ses clients. Elles respectent les exigences ITIL.

Famille ISO 27000 / ISMS ou SGSI

Normes de la famille 27000 pour la mise en place, l'utilisation, la tenue à jour et la gestion d'une politique de sécurité informatique, de sécurité des systèmes d'information ou SGSI (ISMS) : système de gestion de la sécurité de l'information.

ISO 27000 : Série de normes dédiées à la sécurité de l'information
ISO/CEI 27001 : Système de Management de la Sécurité de l'Information (SMSI) — Exigences
ISO/CEI 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information (anciennement ISO/CEI 17799)
ISO/CEI 27003 : Système de Management de la Sécurité de l'Information (SMSI) — Guide d'implémentation

ISO/CEI 27799 : Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

Autres normes

Normes ISO

- ISO/FDIS 31000 : Gestion des risques
- ISO/IEC 38500 : Gouvernance de la sécurité informatique

Normes du British Standards Institution

- BS 25999-1 : BCM, codes de pratique
- BS 25999-2 : BCM, spécifications

Glossaire
INFORMATIQUE

Glossaire
INFORMATIQUE

Adresse IP / Identifiant unique de chaque ordinateur connecté à un réseau (comme Internet). Une adresse IP version 4 est un groupe de quatre nombres (de 0 à 255) séparés par des points (exemple : 109.241.12.154). Le nombre d'adresses est donc « limité » à environ 4 milliards d'adresses. Aujourd'hui, à cause des objets en tout genre connectés à Internet, la pénurie d'adresses en IP V4 dans le monde pousse les acteurs des réseaux à passer en version 6. Cette technologie propose un nombre d'adresses de l'ordre de 3.4 10^38 ce qui est suffisant pour couvrir l'ensemble des éléments connectés à Internet pour quelques années !

Anti-spam / Logiciel mis en place pour filtrer les courriers indésirables et laisser passer les courriers légitimes.

Antivirus / Logiciel de sécurité permettant de détecter tout logiciel potentiellement dangereux pour le système. Son efficacité repose sur sa mise à jour régulière.

Appliance / Elément physique d'un système d'information dédié à une fonction particulière. (Appliance de sécurité de type firewall, Appliance de sauvegarde …).

Avatar / Dans les mondes virtuels, l'avatar est un personnage graphique souvent représenté en 3 dimensions. Personnalisé et contrôlé par l'internaute, il matérialise ce dernier au sein de la communauté virtuelle.

Bande passante / Terme désignant le débit supporté par une ligne de télécommunication. La bande passante peut s'exprimer en Kbps (Kilobit par seconde) ou en Mbps (Mégabit par seconde).

Bit / Abréviation de "Binary Digit", le bit est la plus petite unité d'information gérée par un ordinateur. Ce chiffre binaire peut prendre la valeur 0 ou 1. Il faut 8 bits pour coder un caractère (un octet). A ne pas confondre avec "byte" qui en anglais signifie "octet", soit un groupe de 8 bits.

Botnet / Ou PC Zombie, se dit d'un poste infecté par un malware en attente de sollicitation de la part d'un pirate pour effectuer une attaque de masse.

BYOD (Bring Your Own Device) / Se dit des éléments personnels de type smartphone, tablette, etc. utilisés à des fins professionnelles.

Câblo opérateur / Entreprise disposant d'une infrastructure réseau composée de câble coaxial ou de fibre optique.

Chiffrement / Opération consistant à transformer un message en clair en un message codé compréhensible seulement par la personne disposant du code de déchiffrement. Les navigateurs disposent en standard d'une fonction de chiffrement, comme SSL (Secure Socket Layer), leur permettant de sécuriser, entre autres, les transactions électroniques.

Clé publique / privée / Les techniques de chiffrement actuelles (dites assymétriques) sont basées sur l'utilisation de clés. Le chiffrement d'un document passe par l'utilisation d'une clé appelée « clé publique », car accessible à tous. Le déchiffrement du document nécessite lui l'emploi d'une clé de déchiffrement, dite clé privée.

Codecs / Abréviation de compression/décompression. Dans les domaines du son et de la vidéo numérique, les codecs transforment les flux de données numériques en images et en sons analogiques, et inversement. Ils ont aussi pour mission de réduire la taille des documents et utilisent pour cela de puissants algorithmes de calcul et de compression.

Compression / Opération visant à réduire la taille d'un fichier ou d'un groupe de fichiers. Elle s'effectue au moyen d'un logiciel de compression (7Zip, WinZip, WinRar…) dont le rôle est de coder les informations numériques sous une forme plus compacte. La compression peut être destructive dans le cas d'une image, d'une vidéo ou d'un son, ou non destructive lorsqu'il s'agit de fichiers de données ou d'un logiciel.

Compromission / Un élément du système d'information est dit compromis lorsqu'il a été victime d'un programme malveillant ou d'une intrusion (liée à une faille par exemple).

Cryptographie / Ensemble de techniques « visant à transformer, à l'aide de conventions secrètes, des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse ».

Décryptage / Le décryptage consiste à traduire en clair une information chiffrée dont on ne possède pas la clé : il s'agit donc de « casser » cette dernière. Avec l'évolution des méthodes de chiffrement, le décryptage demande non seulement de solides connaissances en mathématiques, mais aussi des moyens informatiques très importants.

Etat de l'art / Se dit d'une technologie quand elle est appliquée avec les recommandations du concepteur, autrement appelée bonnes pratiques.

Ethernet / Protocole d'échange de données pour certains réseaux locaux. Le débit d'un réseau Ethernet est compris entre 10 et 1 000 Mégabits/seconde. Par extension, désigne tout type de matériel lié à ce protocole (câble Ethernet, carte Ethernet…).

Extranet / Un réseau Extranet consiste à créer des passerelles entre le réseau local Intranet d'une entreprise et les réseaux de ses partenaires, clients et/ou fournisseurs.

Faille / Elément technique ou logiciel comportant un défaut, soit de conception, soit de fabrication, et qui peut être exploité dans un but malveillant.

Favoris (ou "signets") / Cette fonction permet de garder en mémoire l'adresse d'un site ou d'un forum déjà visité afin de ne pas avoir à en ressaisir l'adresse ultérieurement. Très pratiques, les bookmarks permettent de créer son propre carnet d'adresses Web.

Filtrage (logiciel de contrôle) / Logiciel permettant de contrôler l'accès à l'Internet en fonction de certains paramètres (mots-clés, adresses IP…). Les logiciels de surveillance parentale fonctionnent sur le principe du filtrage. Deux modes d'action sont proposés : tout est autorisé sauf ce qui est interdit (liste noire) ou tout est interdit, sauf ce qui est autorisé (principe de la liste blanche). Les techniques évoluent et les listes de filtrage sont plus évoluées permettant ainsi de s'adapter très vite à certains contenus illicites.

Firewall (ou pare-feu) / Dispositif à la fois logiciel et matériel destiné à interdire l'accès d'une personne non autorisée à un réseau local.

Flash / Format d'animation vectoriel utilisé sur l'Internet et popularisé par la société Adobe. La lecture d'animations Flash dans un navigateur nécessite souvent l'emploi de ce plug-in. Il représente souvent une faille et doit être mis à jour très régulièrement. Ce plug-in est en cours d'abandon pour beaucoup de sites au profit de la version 5 du langage HTML qui intègre les composantes multimédia nativement (c'est-à-dire sans ajout de suppléments de programme).

Forum / Espaces de discussion sur Internet, les forums sont de véritables places publiques où chacun peut venir poser des questions, lancer un débat ou répondre aux contributions des internautes.

Fournisseur d'accès Internet (FAI) / Fournisseur d'accès à l'Internet, nommé aussi Provider. Société commercialisant des accès à l'Internet sous forme entre autres d'abonnements.

Freeware / En français "gratuiciel". Logiciel dont l'auteur ne demande aucune rémunération pour son utilisation.

FTP / (File Transfer Protocol). Protocole de Transfert de Fichiers. Cette technologie d'Internet permet de télécharger des fichiers (logiciels, images, documents…) stockés sur des serveurs spécialisés.

GIF / (Graphics Interchange Format). Format de fichier spécialement créé pour la diffusion d'images sur les réseaux. Le GIF produit des images compactes mais limitées à 256 couleurs. Une option de ce format, le GIF animé, permet d'intégrer de petites animations dans des pages Web en vue de les embellir.

Hébergeur / Disposant de serveurs reliés à Internet, l'hébergeur est une société ou un organisme spécialisé dans l'hébergement de sites Web ou d'autres services d'Internet.

Honeypot (pot de miel) / Machine piège mise en place par un administrateur pour attirer les pirates en leur faisant croire que c'est une machine de production. L'administrateur peut ainsi voir l'attaque et analyser la stratégie de l'attaquant (hérité de la maxime de Sun Tzu (l'art de la guerre): Connais ton ennemi).

Implémentation / Mise en place d'un logiciel ou d'une technologie.

Intranet / Réseau local reposant sur les normes, les protocoles et les outils d'Internet : courrier électronique, pages Web, forums… Ce type de réseau est aujourd'hui courant au sein des entreprises ou des établissements scolaires.

Java (langage) / Créé par le constructeur de stations de travail Sun Microsystems, le langage Java a pour mission d'uniformiser et de simplifier la programmation des systèmes informatiques, qu'ils soient PC ou Mac, micro ou super ordinateur, assistants personnels, équipements électroménagers, etc… Parmi les applications de Java, nous trouvons les smartphones, les set top box (ex : box canal satellite), la télévision interactive, les applications embarquées dans les voitures…

Journalisation / Fait d'inscrire dans un journal (ou logs) tous les événements liés à une machine, application, ou Appliance.

Machine cible / Machine sur laquelle on souhaite exécuter un programme (malveillant ou non).

Malware / Petit programme malveillant destiné à extraire des informations de votre ordinateur ou à le transformer en botnet.

Menace active / Tendance du moment sur un type de menace particulière. Début 2016 les principales menaces actives tournaient autour des malwares de chiffrement (cryptolocker).

Modem / Abréviation de modulateur-démodulateur. Périphérique permettant de convertir un signal numérique en signal analogique à modulation de fréquence et vice versa. Le modem permet aujourd'hui aux ordinateurs de communiquer par l'intermédiaire du réseau téléphonique, et par le réseau câblé…

Netiquette / Ensemble de règles de savoir-vivre sur Internet, dictées par la courtoisie et le bon sens. Créé par les premières communautés d'internautes, "Netiquette" est la contraction du mot anglais "net" (réseau) et du mot français "étiquette" (au sens protocolaire du terme).

Numériser / Action de convertir une source analogique (image fixe, vidéo, son) en informations numériques (suite de 0 et de 1). La numérisation des images passe par un scanner, tandis que les sons et les vidéos sont numérisés par des cartes d'acquisition spécifiques.

Octet / En informatique, l'octet est l'unité de mesure standard de la mémoire. Elle représente un groupe de huit bits. Il faut par exemple un octet pour mémoriser un caractère alphanumérique. Les unités de mesure supérieures sont le kilo-octet (Ko), le méga-octet (Mo), le giga-octet (Go), le téra-octet (To) et le Péta-octet (Po).

Phishing / Technique consistant, par une technique ou une autre (mail, faux site internet …), à soutirer des informations de connexion à des comptes utilisateurs (magasin en ligne, banque, compte mail…). Ceci est mis en œuvre par des pirates afin d'usurper l'identité numérique pour effectuer des opérations frauduleuses à l'insu de l'utilisateur et bien entendu à leur profit.

Pilote (driver) / Logiciel destiné à «piloter» un périphérique : imprimante, scanner, modem, lecteur externe… Les pilotes sont généralement fournis par les fabricants avec leur matériel, mais aussi par les éditeurs de systèmes d'exploitation.

Plug-in / Un plug-in (appelé parfois "greffon") est un logiciel qui, une fois installé dans le navigateur, permet à ce dernier d'effectuer des opérations pour lesquellles il n'a pas été conçu : son, vidéo, animation…

PNG / Acronyme de Portable Network Graphics. Format d'image bitmap sur le Web, destiné à remplacer le format GIF. Seuls les navigateurs de dernière génération sont en mesure d'afficher les images PNG insérées dans des pages Web.

Quicktime / Standard de vidéo numérique développé par la société Apple Computer. Sur PC, la lecture de fichiers Quicktime nécessite le logiciel Quicktime pour Windows. Outre la vidéo et le son, Quicktime supporte d'autres types de données, comme les objets et les scènes en 3D. Ce logiciel est abandonné petit à petit au profit de lecteurs plus polyvalents de type VLC.

RAM / Abréviation de Random Access Memory. Mémoire vive d'un ordinateur, composée d'unités de stockage rapides d'accès. On parle aussi de VRam (RAM vidéo) pour les mémoires destinées à l'affichage des images sur le moniteur.

Rebond / Technique d'attaque qui consiste à trouver une machine dans le réseau, moins protégée que les autres (souvent des serveurs de test), pour y pénétrer. L'attaquant peut ainsi « rebondir » sur cette machine pour attaquer le réseau de l'intérieur..

Réseau local / En anglais LAN, Local Area Network. Ensemble d'ordinateurs et de périphériques reliés ensemble au sein d'une structure (câbles, liaison radio…) leur permettant d'échanger des informations entre eux.

Rétention / Se dit du temps maximum de conservation des données lorsqu'une sauvegarde est mise en place. Elle va de quelques heures à plusieurs années en fonction des données.

Routeurs / Tels des échangeurs autoroutiers, ces puissants ordinateurs situés aux carrefours des réseaux acheminent les informations d'une zone d'Internet à l'autre grâce aux adresses IP.

RTC / Réseau Téléphonique Commuté. Appellation technique du réseau téléphonique classique.

Salle blanche / Local technique sécurisé où sont entreposés les serveurs et les éléments réseau d'un système d'information.

Scanner / Périphérique permettant de numériser des documents imprimés, des photos ou des films. La qualité d'un scanner est déterminée par sa résolution (points/pouce) maximale et sa vitesse d'analyse.

Sauvegarde / Action visant à copier et à stocker les données d'un système pour pouvoir les réutiliser en cas de problème.

Serveur (en général) / Ordinateur hébergeant des ressources (informations, images, logiciels…) mises à la disposition d'autres ordinateurs par l'intermédiaire d'un réseau. Sur Internet, on trouve des serveurs de tous types : serveurs Web, serveurs FTP…

Social Engineering / Se dit d'une attaque qui a lieu directement sur l'utilisateur afin de lui soutirer des informations liées au réseau cible de l'attaquant ou dans un but d'extraction de données/argent avec la complicité involontaire de l'utilisateur. La pression psychologique de l'attaquant est souvent la clé de la réussite ainsi que sa très bonne connaissance de sa cible (organigramme, dépendance technique et hiérarchique…).

SPAM / Courriers indésirables et potentiellement infectés de pièces jointes douteuses envoyés en masse.

Streaming / Technologie permettant de lire et interpréter les informations contenues dans un fichier au fur et à mesure de son téléchargement. Certains logiciels permettant par exemple de restituer de la vidéo sur Internet fonctionnent en streaming : le film se joue à l'écran alors que le fichier de la vidéo n'est pas entièrement téléchargé.

Surface d'attaque / Se dit du spectre des possibilités pour un attaquant de compromettre un réseau. Plus la surface est étendue (faible sécurité) plus l'attaque s'en trouvera facilitée. La réduction de la surface d'attaque se fait donc en durcissant la sécurité à tous les niveaux du système d'information.

TCP / IP / (Transmission Control Protocol/Internet Protocol). Ce protocole universel définit le format des données transmises sur Internet ainsi que l'adressage hiérarchique des ordinateurs. Ce protocole permet également de contrôler que les données transmises soient toutes bien reçues par le destinataire.

Tiers de confiance / Société dont la mission est de garantir la sécurité et le bon déroulement des transactions sur le Web. Reconnu par les banques et les commerçants, le tiers de confiance prend à sa charge la facturation et le règlement des commandes passées par les internautes sur les sites Web marchands.

Transfert de fichiers / Technique consistant à transférer des fichiers d'un ordinateur vers un autre. Sur Internet, le transfert de fichiers s'appuie sur des serveurs utilisant le protocole "FTP" (File Transfert Protocol). Le transfert s'effectue à l'aide du navigateur ou d'un logiciel spécialisé.

URL / (Uniform Resource Locator) Adresse électronique permettant d'identifier un site, un service ou un fichier sur le World Wide Web.

Virus / Elément malveillant installé à l'insu de l'utilisateur visant à perturber, voire à empêcher le fonctionnement de son système. Les virus sont de moins en moins répandus au profit de menaces plus interactives.

Association Nationale des Directeurs
et Directeurs-Adjoints des Centres De Gestion
de la Fonction Publique Territoriale

LES COLLECTIVITÉS TERRITORIALES FACE À LA *cybercriminalité*

Les enjeux de la sécurité informatique sont aujourd'hui nombreux et les collectivités territoriales doivent faire face à des menaces liées à l'utilisation des outils informatiques et à la dématérialisation de certaines procédures : intrusions, vols d'informations (état-civil, plateforme marchés publics, fichiers scolaires et périscolaires…). Les conséquences peuvent être lourdes en termes de protection des données et de gestion des services.

Se trouvant démunies de repères dans la gestion des risques informatiques et face à des utilisateurs parfois imprudents, les collectivités investissent dans des protections très couteuses ou bien n'ont pas réellement conscience des répercussions, alors que des solutions simples peuvent être mises en place.

Aussi, l'ANDCDG a souhaité mettre à leur disposition un guide leur permettant d'avoir une approche pragmatique et globale, que le lecteur soit élu ou agent territorial, de tous les risques encourus, des bonnes pratiques à adopter, ainsi que des solutions en terme d'assurance et de protection juridique.

L'ANDCDG tient à remercier les experts en matière de sécurité informatique qui ont contribué à la rédaction de ce guide et pour l'enrichissement qu'ils y ont apporté : Stéphane Dahan, Responsable Sécurité Informatique et des Réseaux chez Securiview, Frédéric Gard, Responsable Pôle Santé chez Gras Savoye et Rémy Février, Maître de Conférences au CNAM, Responsable des Unités d'Enseignement « Management et Audit des Systèmes d'Information », ancien Lieutenant-Colonel de la Gendarmerie Nationale.

www.andcdg.org / Contact
Secrétariat ANDCDG - 15, rue Boileau - 78008 VERSAILLES Cedex
e-mail : andcdg@cigversailles.fr - Téléphone : 01 39 49 63 10 - Fax : 01 39 49 63 13

EN PARTENARIAT AVEC :
GRAS SAVOYE
Willis Towers Watson