Sujet national pour l'ensemble des centres de gestion organisateurs

INGENIEUR TERRITORIAL

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE

SESSION 2014

Etablissement d'un projet ou étude portant sur l'option choisie par le candidat au moment de son inscription.

Durée : 4 heures
Coefficient : 5

INFORMATIQUE ET SYSTEMES D'INFORMATION

OPTION : RESEAUX ET TELECOMMUNICATIONS

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.

- Aucune référence (nom de collectivité, nom de personne, ...) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.

- Seul l'usage d'un stylo soit noir soit bleu est autorisé (bille à encre non effaçable, plume ou feutre). L'utilisation d'une autre couleur pour écrire ou souligner sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.

- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 17 pages
Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué

- Vous préciserez le numéro de la question et le cas échéant de la sous-question auxquelles vous répondrez.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas...

Vous êtes nouvellement recruté comme Directeur des systèmes d'information et télécommunications de la ville d'Ingéville (15 000 habitants). Le Maire et le Directeur général des services vous remettent un état des lieux succinct des systèmes d'information de la ville (Document 1).
Ces dernières années, de nombreux projets ont été menés, en termes d'acquisition de progiciels métiers, de développements Web (Site Intranet), de services aux administrés (Portail citoyens). Un aspect important a toutefois été négligé, celui de la sécurité informatique, qui, par conséquent, sera un axe prioritaire de vos missions.

Question 1 (6 points)

En utilisant vos connaissances techniques personnelles, vous exposerez d'une manière synthétique les quatre grands principes qui régissent la sécurité des systèmes d'information. Pour chacun des principes, vous illustrerez par un exemple que vous avez ou auriez pu rencontrer dans votre environnement professionnel.
Vous veillerez à ne pas citer de nom de collectivité.

Question 2 (14 points)

En partant de l'état des lieux actuel des systèmes d'information d'Ingéville, en vous aidant de certains éléments du dossier et en exploitant vos connaissances techniques personnelles, vous décrirez les grandes étapes techniques, opérationnelles et méthodologiques du projet de refonte de la sécurité des systèmes d'information qui vous a été confié. Ce projet, qui concerne évidemment le site principal (Hôtel de ville), doit également englober la sécurité d'un site distant que vous avez la charge d'interconnecter (voir document 1).

Liste des documents joints

Document 1 :	État des lieux des systèmes d'information d'Ingéville – 2 pages.
Document 2 :	L'école des Beaux-Arts de Paris externalise sa sauvegarde - *ZDnet.fr.*- 2 pages
Document 3 :	10 conseils pour la sécurité de votre système d'information - *CNIL – Fiche pratique* – 3 pages
Document 4 :	Protéger ses systèmes d'information en misant sur la sensibilisation - *La gazette* – juillet 2013 – 1 page
Document 5 :	Le réseau privé virtuel expliqué à votre directeur général - *01 Business & Technologies* – novembre 2012 – 1 page
Document 6 :	Vérifier sa sécurité informatique pour éviter tout souci juridique - *01 Business & Technologies* – décembre 2012 – 1 page
Document 7 :	Les dix fonctionnalités essentielles de votre futur firewall *Extraits de :* **De la défense périmétrique à la défense en profondeur - BSSI.fr* – avril 2013 **Les 10 fonctionnalités essentielles de votre futur firewall – aucœurdesinfras.fr* – mai 2013 – 2 pages
Document 8 :	Les bénéfices de la Virtualisation des serveurs en termes de sécurité - www.virtu-all.fr. - site consulté en janvier 2014 – 1 page
Document 9 :	L'informatique démunie face aux catastrophes naturelles - *01 Business & Technologies* – novembre 2012 – 1 page.

Documents reproduits avec l'autorisation du CFC

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet

DOCUMENT 1

Etat des lieux des systèmes d'information de la ville d'Ingéville.

Données générales :

- 100 utilisateurs en réseau.
- Actuellement, tous les utilisateurs sont regroupés sur le même site (Hôtel de ville).

Equipe informatique :

- Vous encadrez 2 techniciens informatiques.

Salle serveurs / équipement réseau:

- 8 serveurs (Windows server 2003 et 2008) répartis comme suit :
- Un serveur de messagerie (exchange 2003)
- Un serveur de fichiers, contrôleur de domaine (Windows server 2008 / Active Directory)
- 6 serveurs qui hébergent les divers progiciels métiers, le site intranet, le logiciel antivirus.
- Un firewall CISCO PIX 515e, installé en 2003.
- Une solution anti-spam (boitier), installée à la même époque que le firewall.
- Une solution libre de filtrage URL, peu satisfaisante.
- Un accès SDSL de 1Mbit/s (débit maximum possible pour l'instant, pas d'éligibilité à la fibre optique).
- Pas de proxy.
- Pas de virtualisation.

Progiciels et applications :

- Un portail citoyen propriétaire, hébergé chez l'éditeur, interfacé avec les logiciels métiers (enfance, état-civil...)
- Divers progiciels métiers (Finances – Ressources Humaines – Etat Civil – Enfance et petite enfance – Urbanisme – Logement, etc.), la plupart en version full Web, Bases de données Oracle (V 11g).

Données complémentaires

- Seuls les fichiers des utilisateurs (serveur de fichiers) sont sauvegardés tous les soirs sur cartouches via un lecteur de sauvegarde LTO 4. Volumétrie approximative 200 Go.
- Autres données volumétriques :
  - Ensemble des bases de données : 5 Go
  - Base de données Exchange (mails) : 90 Go (75 Go il y a un an)
  . Ensemble des données systèmes des serveurs : 220 Go
- Pas de PRA (plan de reprise d'activité).

- Les stratégies de groupe (GPO) sont utilisées au minimum.

Interconnexion du nouveau site distant

- Le nouveau site accueillera 6 agents de la ville qui auront besoin de se connecter au système d'information (messagerie, logiciel de gestion des finances, intranet etc.).
- Le site est distant de 800 mètres. Les toits des deux bâtiments sont à vue. Pour des raisons budgétaires (trop de travaux de voirie), il n'est pas envisageable de déployer une connexion en fibre optique. La solution « ligne spécialisée opérateur », n'a pas été retenue.

DOCUMENT 2

L'école des Beaux-Arts de Paris externalise ses sauvegardes

Source : ZDnet.fr

Jugeant contraignant le maintien d'une infrastructure en interne, l'école nationale supérieure des Beaux-Arts de Paris a externalisé les sauvegardes de l'ensemble de ses serveurs.

«Lorsque notre librairie de cartouches à bandes est tombée en panne, j'ai réalisé à quel point notre infrastructure de sauvegarde était complexe et fastidieuse à gérer et à maintenir. « Surtout pour une petite équipe comme la nôtre», se souvient Torsten Westphal, responsable informatique de l'École nationale supérieure des beaux-arts de Paris (ENSBA). Cette fonction technique est d'autant plus critique que le site de l'école, dans un quartier historique, est très fragile. Facilitée par le fait que la librairie de cartouches était louée, la décision est alors prise d'externaliser les sauvegardes de tous les serveurs auprès d'un prestataire. Les postes clients ne sont pas concernés, puisque toutes les données des utilisateurs sont stockées sur des serveurs.

Sauvegarde de bases ouvertes

Après un rapide tour du marché, le fournisseur Backup Avenue est retenu. «C'était le seul acteur capable de sauvegarder des bases de données Exchange ouvertes», précise Torsten Westphal, rassuré par le fait que ce service était basé sur un logiciel réputé – Tivoli Storage Manager d'IBM. Un test est réalisé avec la sauvegarde d'un ensemble de fichiers pesant 500 Mo. Il se révèle concluant. La solution est donc déployée sur les cinq machines sous Windows Server 2003: une base Exchange d'environ 40 Go, deux serveurs de fichiers, un serveur de services techniques (dont un annuaire Active Directory), ainsi qu'un serveur de bases de données exécutant Sybase, SQL-Server et des moteurs propriétaires.

Ce déploiement a nécessité l'ouverture d'un port sur le pare-feu (firewall) et l'installation d'un agent Tivoli sur chacun de ces serveurs. «Nous les avons téléchargés et installés nous-mêmes, excepté l'agent Exchange qui a imposé l'intervention sur site d'un ingénieur de Backup Avenue», précise Torsten Westphal. Il a également fallu préciser, via un portail web, les données qui devaient être mises à l'abri. Par exemple, un filtre a permis de restreindre les sauvegardes des fichiers aux données bureautiques et, pour les images, à certains répertoires.

200 Go copiés via un lien SDSL

Les flux de sauvegarde passent par la connexion internet standard de l'école - un lien SDSL à 2 Mbit/s. Malgré l'absence de gestion intelligente de la bande passante, les applications ne sont jamais handicapées puisque les transferts ne sont effectués que la nuit et le week-end. Du lundi au vendredi, les agents se connectent en effet chaque nuit au service Backup Avenue et effectuent des copies incrémentales – seuls les blocs de données modifiés sont transférés. Et le week-end, l'ensemble des 200 Go de données est envoyé. L'ENSBA dispose encore d'un peu de marge, puisqu'elle a négocié un espace de 250 Go, pour un coût de 1.345 € par mois (auquel se sont ajoutés des frais de licence et de mise en œuvre). «Le danger d'un tel service, c'est que l'on finit par l'oublier, alors qu'il faut quand même surveiller la volumétrie», prévient Torsten Westphal.

Restaurations nécessaires

Plusieurs restaurations ont dû être effectuées suite à des pertes de données sur des fichiers bureautiques et des bases de données. La plus grosse restauration, qui n'a pas dépassé 800 Mo, a été réalisée en 45 minutes. «La base Exchange est beaucoup plus volumineuse. Si elle devait être restaurée, Backup Avenue nous l'enverrait sur DVD-Rom, par coursier», affirme Torsten Westphal. Et d'ajouter: «nous apprécions particulièrement la possibilité de

configurer les sauvegardes à partir de n'importe quel PC, même à l'extérieur de l'école. Cela se révèle très utile, par exemple en cas d'absence de l'administrateur.»

Les délais liés à la restauration d'images système, ainsi que leur nature particulièrement critique, sont toutefois perçus comme la principale limite de l'externalisation. «C'est pourquoi nous allons déployer un outil de sauvegarde qui permettra de conserver chez nous ces images tout en les transmettant à Backup Avenue», prévoit Torsten Westphal.

DOCUMENT 3

10 conseils pour la sécurité de votre système d'information

CNIL.

Fiche pratique

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

1. Adopter une politique de mot de passe rigoureuse

L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections. Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support. La DSI ou le responsable informatique devra mettre en place une politique de gestion des mots de passe rigoureuse : un mot de passe doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois). Le système doit contraindre l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment. Généralement attribué par l'administrateur du système, le mot de passe doit être modifié obligatoirement par l'utilisateur dès la première connexion. Enfin, les administrateurs des systèmes et du réseau doivent veiller à modifier les mots de passe qu'ils utilisent eux-mêmes.

2. Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2...), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes « génériques » ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

3. Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum); les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné. Par ailleurs, le contrôle de l'usage des ports USB sur les postes « sensibles », interdisant par exemple la copie de l'ensemble des données contenues dans un fichier, est fortement recommandé.

4. Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné. Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

5. Veiller à la confidentialité des données vis-à-vis des prestataires
Les interventions des divers sous-traitants du système d'information d'un responsable de traitement doivent présenter les garanties suffisantes en termes de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès. La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance. Les éventuelles interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre. Les données qui peuvent être considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un chiffrement.

« A noter » : l'administrateur systèmes et réseau n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Pourtant, il a besoin d'accéder aux plates-formes ou aux bases de données pour les administrer et les maintenir. En chiffrant les données avec une clé dont il n'a pas connaissance, et qui est détenue par une personne qui n'a pas accès à ces données (le responsable de la sécurité par exemple), l'administrateur peut mener à bien ses missions et la confidentialité est respectée.

6. Sécuriser le réseau local
Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc. Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents. La messagerie électronique doit évidemment faire l'objet d'une vigilance particulière. Les connexions entre les sites parfois distants d'une entreprise ou d'une collectivité locale doivent s'effectuer de manière sécurisée, par l'intermédiaire des liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel). Il est également indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc. Enfin, les accès distants au système d'information par les postes nomades doivent faire préalablement l'objet d'une authentification de l'utilisateur et du poste. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS.

7. Sécuriser l'accès physique aux locaux
L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc. La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

8. Anticiper le risque de perte ou de divulgation des données
La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie. Il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé. Les serveurs hébergeant des données sensibles ou capitales pour l'activité l'organisme concerné doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence – secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur. Les supports nomades (ordinateurs portables, clé USB, assistants personnels etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, au regard de la sensibilité des dossiers ou documents qu'ils peuvent stocker. Les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent

être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

9. Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des agents ou des salariés. Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information. Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'organisme concerné. Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine. Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données. Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet. Ce document devrait également rappeler les conditions dans lesquelles un salarié ou un agent peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord de son responsable, du service juridique ou du CIL de l'entreprise ou de l'organisme dans lequel il travaille.

DOCUMENT 4

Protéger ses systèmes d'information en misant sur la sensibilisation

Aisne • 540 500 hab.

Exemplaire pour sa sécurité informatique, le conseil général de l'Aisne travaille activement à transmettre le «virus» de la sécurité à tous les maillons de la collectivité.

Jeu de l'oie géant contre cyberattaques. Pour sensibiliser les agents à la problématique de la protection des données numériques, le conseil général mise depuis plusieurs années sur des formations ludiques et didactiques. Jeu de rôle, QCM, formation et articles sur les dangers d'internet ou e-formation par le biais de saynètes, tous les moyens sont bons pour réussir à transformer agents et élus en chevalier défenseur de la forteresse des systèmes d'information de la collectivité.

Responsabilité engagée

«Nous avons les problématiques d'une multinationale avec 126 métiers différents qui réclament des niveaux de sécurité et de disponibilité très personnalisés. Le risque est réel et la responsabilité des élus clairement engagée. Or il est impossible de bâtir une politique s sécuritaire fiable sans le concours de tous. Les contraintes doivent être comprises et acceptées pour ne pas être contournées », explique Hervé Fortin. Le responsable de la sécurité des systèmes d'information (SSI) du conseil général de l'Aisne se démène donc pour sensibiliser à tous les échelons. «En 2009, par exemple, j'ai lancé un jeu concours. 500 utilisateurs sur les 1200 connectés au réseau [1800 agents au total à l'époque] y ont participé. Aujourd'hui, environ 90% des agents ont bénéficié au moins d'une formation en salle avec moi et un outil d'e-formation performant permet de compléter ces temps collectifs. Il faut compter trois ans pour voir évoluer les comportements», estime-t-il. Filtre antispams, diminution de l'utilisation d'internet, mots de passe et autres mesures de prévention sont désormais moins vécues comme des restrictions de liberté. «Les personnes n'arrivent plus en hurlant quand un site est bloqué. Bien connaître chaque métier est primordial. S'il est normal qu'un agent du service "enfance" puisse avoir à se renseigner sur des sites traitant de sexualité enfantine, cela peut être problématique pour un agent de la voirie», illustre le responsable de la SSI pour qui la meilleure solution consiste à mener de front sensibilisation et mise en place des outils techniques. Hervé Fortin précise que pour réussir cette politique, il est indispensable d'instaurer une charte informatique: «La politique générale de sécurité doit être écrite de façon succincte, pas trop technique et juridiquement viable. En outre, elle doit bénéficier d'un soutien actif de la direction, des élus et des représentants des salariés.» Login et mot de passe personnel sont de rigueur afin d'accéder à un espace de travail personnalisé. Toutes les sauvegardes se font en réseau de façon chiffrée à deux endroits physiques différents», précise Hervé Fortin.

Quarantaine

En matière de spams, la collectivité applique un filtre très strict avec un système de quarantaine sur lequel les agents peuvent aller consulter, si besoin, les messages litigieux. «Sur les deux millions de mails reçus ces trente derniers jours, seuls 10% n'étaient pas des spams! Notre politique de blocage a donc permis d'éviter 8142 heures de navigation inutile », informe Hervé Fortin qui estime à 100000 euros par an le budget de prestations externes liées aux questions de sécurité informatique. L'Aisne reste malheureusement une exception; regrette son homologue au conseil régional du Nord-Pas-de-Calais, Thierry Henniart. La sécurité des systèmes d'information sont encore trop souvent confinée au niveau technique.»

Les outils nomades sous contrôle

«Le risque de pertes de données, lié ou non à de la malveillance, s'est considérablement amplifié quand les encadrants sont devenus mobiles. Pour que ces derniers acceptent les contraintes, il faut qu'ils aient pris conscience de ce risque», souligne Hervé Fortin, responsable de la sécurité des systèmes d'information de l'Aisne. La collectivité a choisi d'équiper elle-même ses encadrants et de bannir leurs appareils personnels: «Ceux-ci représentent une grosse faille sécuritaire et reviennent beaucoup plus chers en termes de suivi et de maintenance.» Pour les agents en télétravail, la collectivité a choisi le bureau virtuel. «Tout se passe comme si la personne avait seulement devant elle un écran de visualisation déporté», détaille Hervé Fortin.

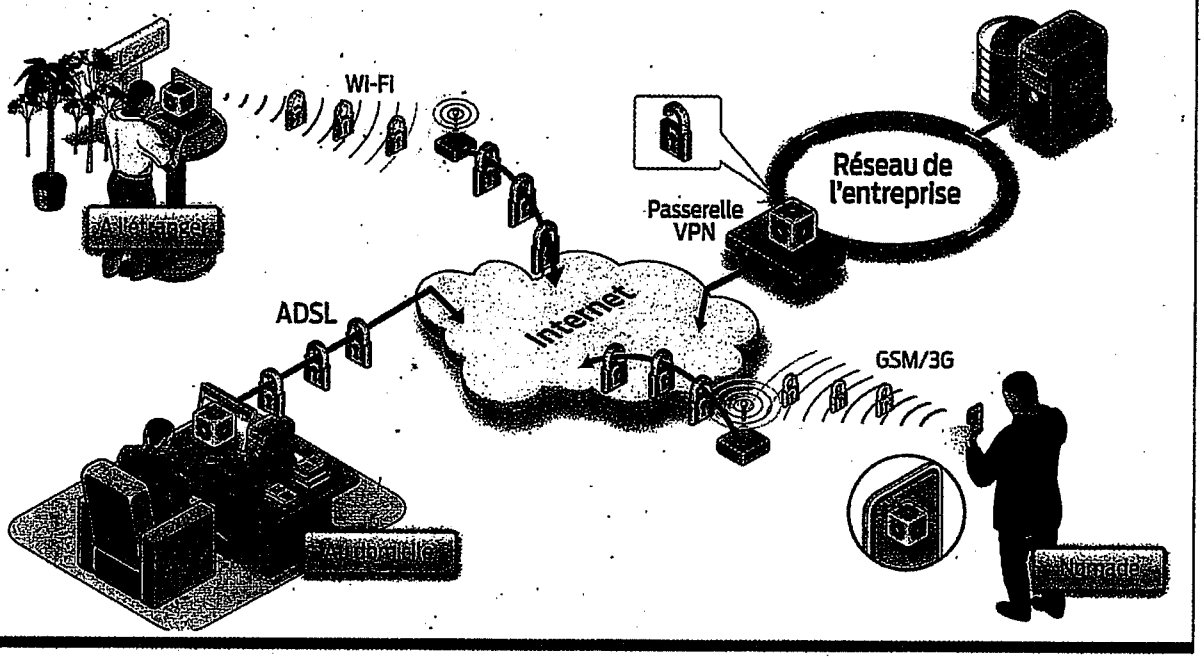
DOCUMENT 5

Le réseau privé virtuel expliqué à votre directeur général

POURQUOI S'Y INTÉRESSER ?

Se connecter au réseau de l'entreprise depuis l'extérieur expose le système d'information à de gros risques. Les réseaux privés virtuels servent à établir une passerelle sécurisée et fiable.

SÉCURISER LES LIAISONS AVEC LES DIFFÉRENTS LIEUX EXTÉRIEURS À L'ENTREPRISE



Les gains

1. Une connexion chiffrée.

Les réseaux privés virtuels (VPN pour Virtual Private Network) utilisent des protocoles réseaux afin d'encapsuler les données véhiculées via des techniques de chiffrement (L2TP, SSH, SSL/TLS, etc.). Impossible pour un pirate d'opérer une écoute : les données sont protégées.

2. Un accès universel.

Les connexions sont possibles depuis n'importe quel type de terminal sans restrictions. Soit à l'aide d'un client logiciel, soit grâce à une fonctionnalité déjà présente dans le système d'exploitation (comme sur iOS). Les collaborateurs accèdent ainsi à des données sensibles sans exposer l'entreprise à un vol d'informations.

3. Une technologie peu coûteuse

La connexion se fait via internet; à savoir par une liaison d'accès au réseau local non fiable. A part l'achat de passerelles connectées au cœur de réseau et éventuellement, de licences d'applications clientes, le VPN établit une connexion externe sécurisée à moindre coût.

Les limites

1. Des protocoles vulnérables.

SSL, par exemple, s'est vu malmené et cassé à plusieurs reprises. Il faut donc s'assurer que la technique de chiffrement qui sert à encapsuler les données est bien à jour, afin d'éviter de rendre caduque la sécurisation du dispositif.

2. Une qualité de service moyenne.

Les réseaux privés virtuels n'offrent pas la qualité de service des lignes spécialisées de type X25 (supprimée récemment), MPLS ou Swift (pour les banques).Ces solutions étant les plus sécurisées puisque les «tuyaux» qui véhiculent les données sont dédiés à l'entreprise.

3. Des précautions à prendre.

La mise en place d'un VPN n'exclut pas le respect des principes de sécurité de base comme la génération d'un mot de passe complexe et changé régulièrement; la vérification des habilitations pour éviter les accès à partir d'un compte censé être désactivé; ou encore le suivi des logs pour s'assurer qu'aucune sortie anormale n'a eu lieu.

DOCUMENT 6

Vérifier sa sécurité informatique pour éviter tout souci juridique

Audit : la moitié des entreprises ne procèdent pas à une analyse des risques

L'audit permet une mesure précise du risque juridique et d'établir un plan de mise en conformité

Empiler les couches de sécurité ne suffit pas à s'assurer une couverture légale en cas d'incident informatique. Dans le cadre de la protection des données personnelles, d'informations liées au secret des affaires ou relevant d'un enjeu de propriété intellectuelle, l'entreprise ne peut se contenter de s'appuyer sur une défense matérielle et logicielle: il lui faut également disposer d'un arsenal juridique. Voilà pourquoi effectuer un audit juridique de son système d'information (SI) s'avère indispensable. Et plus particulièrement au niveau de la partie sécurité. « *Cet audit, réalisé à partir d'un référentiel légal et métier de règles, vise à cartographier les risques juridiques encourus par l'entreprise et ses dirigeants* », explique Arnaud Tessalonikos, avocat associé au sein de Courtois-Lebel.
Faute de s'en être occupée, l'entreprise risque de se retrouver démunie en cas de poursuites judiciaires. Même bien équipée, elle serait, dans le meilleur des cas, taxée de négligence.

Déployer des outils de traçabilité

« *Les sociétés doivent protéger leurs propres informations ou celles qu'elles détiennent sur les autres entreprises. L'ampleur de la protection requise dépendra ensuite de la sensibilité plus ou moins grande des informations concernées. Les données relatives à l'état de santé des collaborateurs, à leur situation financière ou familiale, par exemple, constituent des informations sensibles, donc spécifiquement protégées par la loi* », explique Arnaud Tessalonikos. Assurer la protection de l'entreprise d'un point de vue juridique se traduit essentiellement par le déploiement d'outils de traçabilité : qu'il s'agisse d'accès au système d'information ou des communications passées, des transferts de fichiers, etc. Lors de cet audit, l'entreprise et les pratiques de ses dirigeants sont évaluées point par point, ce qui permet de disposer d'une mesure précise du risque juridique, mais aussi d'un plan d'actions de mise en conformité.

Ce dernier prend en compte la « criticité » des données et des applications concernées, afin de fixer des priorités. « *Une fois le* SI *certifié conforme, l'une des étapes fondamentales de la démarche consiste à se doter d'un arsenal d'outils juridiques opérationnels, comme une charte d'utilisation du système d'information, afin de maintenir cette conformité dans la durée* », ajoute Arnaud Tessalonikos. Un point à ne pas négliger si l'on considère les évolutions rapides des entreprises modernes et le niveau élevé de complexité de certaines organisations.

Contrôler les contrats passés avec les prestataires

Enfin, il convient de rester vigilant lors des phases de contractualisation avec des tiers ou des fournisseurs. « *En ce moment,* je *m'occupe d'un client évoluant dans le secteur de l'assurance, qui passe à la voix sur IP. Il a omis de spécifier dans le contrat signé avec son prestataire les règles de sécurité propres à son entreprise, en matière de contrôle d'accès notamment. Conséquence, le fournisseur n'est pas obligé de respecter* ces *règles. Ce qui s'avère plutôt ennuyeux, d'autant que pour s'y conformer, il veut réviser ses tarifs* », raconte Arnaud Tessalonikos. Idéalement, ces règles auraient dû être énoncées en amont lors de l'appel d'offres.

DOCUMENT 7

Les dix fonctionnalités essentielles de votre futur firewall

Les firewalls ou pare-feu sont un élément essentiel de la protection du système d'information. Première barrière pour protéger le réseau des attaques externes, cet élément historique de la sécurité du SI a connu de nombreuses évolutions technologiques depuis les quinze dernières années. Ainsi le pare-feu qui était au départ une simple protection périmétrique, est devenu un élément parmi un ensemble plus vaste qu'on peut qualifier de défense en profondeur du système d'information.

Un bref historique

Au commencement étaient les routeurs filtrants, avec des routeurs réseaux qui permettaient d'effectuer un simple filtrage au niveau 3 du modèle OSI, c'est à dire au niveau IP, ainsi que partiellement au niveau 4 (connexions TCP) par le moyen de listes de contrôles d'accès (ACL).

Puis sont apparus des pare-feu plus évolués, qui gèrent l'ensemble des protocoles réseaux de niveau 3 et 4 (protocoles de routage, TCP, UDP).

Enfin une petite révolution fut l'avènement des statefull firewalls, c'est à dire des pare-feu gardant une table d'état des connexions TCP actives. Cela permit d'établir des règles de sécurité dynamiques, en rejetant les paquets qui ne correspondent pas à des connexions déjà établies.

Un élément incontournable de la sécurité périmétrique...

Aujourd'hui le pare feu est l'un des éléments essentiels de la sécurité réseau. Tous les principaux pare-feu du marché sont statefull, gèrent le niveau 3 et 4, et apportent ainsi un premier niveau de défense périmétrique. Un pare-feu permet :

- De dissimuler la topologie du réseau et les services vulnérables.
- De différencier le trafic entrant et sortant.
- De délimiter des zones de confiance: réseau local, DMZ...
- De constituer un point d'accès distant pour l'interconnexion des réseaux d'entreprise par les connexions VPN IPSEC.

Il est utile de rappeler que les règles de sécurité implémentées sur un pare feu doivent être le résultat d'une politique de sécurité, et non pas l'inverse ! Il est nécessaire au préalable d'effectuer une analyse de risque qui va conduire à déterminer la criticité des ressources, les menaces potentielles et le niveau de risque résiduel.

Dans la pratique, on voit souvent les règles de sécurité d'un pare-feu s'additionner dans le temps jusqu'à parfois devenir obsolètes. Il est donc important d'auditer ces règles régulièrement, par exemple tous les 6 mois, pour s'assurer qu'elles sont toujours en accord avec la politique de sécurité.

UTM ou l'empilement des services

La réponse des fabricants de pare-feu pour lutter contre les nouvelles menaces a été l'UTM : Unified Threat Management. Derrière ce terme marketing on trouve en fait la possibilité de filtrer les paquets jusqu'au niveau 7 (applicatif) du modèle OSI. En analysant le trafic à la

volée, et en le comparant à des bases de signature ou des modèles heuristiques, UTM permet d'accumuler sur un unique point du réseau les services suivants :

- Filtrage au niveau IP et transport
- Filtrage applicatif avec analyse du trafic HTTP, FTP, VoIP, P2P...
- IPS (Intrusion Prévention system) qui va détecter ou bloquer les attaques connues à partir d'une base de signature
- Antivirus et Antispam
- Filtrage des URLs

Les dix points clés indispensables à votre firewall de nouvelle génération.

1-Votre prochain firewall doit identifier et contrôler les applications sur n'importe quel port, pas seulement les ports standard (y compris les applications utilisant http ou d'autres protocoles).

2-Votre prochain firewall doit identifier les techniques d'évasion et les contournements : proxy, accès distant, applications dans un tunnel chiffré.

3-Votre prochain firewall doit déchiffrer les flux SSL sortants

4-Votre prochain firewall doit permettre un contrôle des différentes fonctions d'une même application (ex. : SharePoint Admin face à SharePoint Docs)

5-Votre prochain firewall doit détecter les menaces dans les applications collaboratives autorisées (ex. : SharePoint, Box.net, MS Office Online...)

6-Votre prochain firewall doit gérer le trafic inconnu avec des règles et ne pas simplement les laisser passer

7-Votre prochain firewall doit identifier et contrôler les applications partageant une même connexion

8-Votre prochain firewall doit disposer du même contrôle et de la même visibilité sur les utilisateurs distants que sur les utilisateurs internes

9-Votre prochain firewall doit simplifier la sécurité réseau. Pouvoir contrôler les applications ne doit pas ajouter de complexité.

10-Votre prochain firewall doit fournir le même débit et les mêmes performances malgré l'activation de tous les contrôles applicatifs.

Conclusion

On voit que les pare feu qui ne proposaient au départ qu'un filtrage de niveau 3 et 4 sont devenus beaucoup plus complets et peuvent maintenant effectuer un filtrage à tous les niveaux du modèle OSI, et en particulier aux niveaux 6 et 7 pour permettre la terminaison SSL et l'analyse de protocoles.

Au-delà du rôle classique de protection périmétrique et de terminaison VPN qui reste essentiel, on trouve maintenant toute une gamme d'équipements qui vont permettre d'implémenter les concepts de défense en profondeur.

DOCUMENT 8

Les bénéfices de la virtualisation des serveurs en termes de sécurité

Les bénéfices de la virtualisation sont tellement évidents que de nombreuses organisations l'ont rapidement adoptée et déployée en production sans parfois prendre le temps d'analyser toutes les implications de sécurité spécifique à cette technologie.

Parmi les bénéfices immédiats de la virtualisation des serveurs on peut entre autres identifier les points suivants :

- Isolation
- Retour arrière
- Portabilité

La possibilité de configurer des réseaux dédiés permet aux administrateurs de réduire les risques liés à la propagation d'une infection.

Si un programme malicieux est installé dans une machine virtuelle, il est relativement facile de la restaurer à un état précédemment sain. Même si cela n'est pas toujours possible, ceci est particulièrement utile dans le cas de machine virtuelle hébergeant des données statiques comme les serveurs web.

La relative isolation qui existe entre une machine virtuelle et le serveur hôte permet de limiter significativement les dégâts causés par des programmes malicieux destinés à corrompre les données d'un système.

Quand bien même le disque virtuel est totalement corrompu, le disque physique sur lequel il est hébergé reste intact.

La portabilité des machines virtuelles offre la possibilité de mettre en œuvre des processus de restauration et de PRA à moindres coûts et réduit considérablement le temps nécessaire à la remise en route d'un serveur. Elle permet entre autres de déplacer facilement la charge de travail d'un serveur physique à un autre.

De nombreuses solutions permettent de déplacer cette charge de travail dans toutes les directions indépendamment des configurations matérielles :

- Physique vers Virtuelle (P2V)
- Virtuelle vers Virtuelle (V2V)
- Virtuelle vers Physique (V2P)

Les nouvelles fonctions offertes par la virtualisation permettent de concevoir des systèmes capables de basculer automatiquement en cas de défaillance. Enfin, en consolidant des infrastructures complexes dans des environnements et des réseaux virtuels séparés, les administrateurs peuvent configurer des règles spécifiques à chaque environnement et maximiser la sécurité. (Environnements de tests, ou de développement, environnements de production).

DOCUMENT 9

L'informatique démunie face aux catastrophes naturelles

JEAN-PHILIPPE SANCHEZ, consultant technique chez Netiq, a profité de la Journée internationale de la prévention des catastrophes[1] pour tirer une conclusion sévère sur l'incapacité de l'informatique à lutter contre les catastrophes naturelles.

Il y a quelques mois, au nord de l'Italie, un puissant séisme ravageait une partie du territoire, balayant de nombreuses structures et infrastructures. Des bâtiments publics, notamment, furent touchés. La perte des données des administrés était passée en pertes et profits. Quelques semaines plus tard, le législateur italien a cependant estimé, au détriment de ces collectivités, que ces dernières étaient responsables des informations qu'elles hébergeaient. Constatant par la même occasion l'absence quasi totale de plan de reprise d'activité (PRA) pour ces institutions, une loi allait du coup les enjoindre à en élaborer un. Un exemple qui démontre cette triste fatalité : l'informatique ne peut pas faire grand-chose contre les catastrophes naturelles.

Plus de 40 % des entreprises restent fermées après un sinistre

Le rôle de l'informatique consiste pourtant à tout mettre en œuvre pour que les systèmes d'information soient prêts à se remettre en service après une telle catastrophe, en en contenant au maximum les effets. La question à se poser est donc de savoir quand un désastre va se produire plutôt que s'interroger sur l'éventualité qu'un tel événement survienne. A titre d'exemple, selon le département du Travail américain, plus de 40% des entreprises restent fermées à la suite d'un sinistre. Et parmi celles qui tiennent bon, au moins 25 % finissent par cesser leur activité dans les deux années qui suivent. Mais si l'importance d'une vaste stratégie de reprise sur sinistre ne soulève guère de doutes, pourquoi toutes les sociétés' n'en déploient-elles pas une? Deux réponses à cette question. La première porte sur les efforts. A l'époque où toutes les données importantes étaient sauvegardées sur des serveurs, le contenu de ces serveurs était lui-même sauvegardé sur des bandes. Les bandes étaient certes peu onéreuses (ce qui est toujours le cas), mais de nombreuses entreprises ont estimé que leur capacité restait limitée et que leur gestion empêchait de les déplacer vers des sites de stockage distants.
Procéder à des contrôles aléatoires pose également trop de problèmes. Cette tâche mobilise un nombre d'employés excessif et prend une trop grande partie de leur temps. De plus, en cas de catastrophe, des données sont tout de même perdues. La seconde raison qui empêche les entreprises à mettre en place un plan de reprise sur sinistre est liée aux investissements qu'impliquent de telles initiatives, et notamment aux coûts des technologies telles que la réplication des serveurs (server mirroring) et les grappes de serveurs (le clustering). Ces techniques assurent, certes, une restauration quasi instantanée sans intervention manuelle, mais au prix d'une duplication intégrale de l'infrastructure. De fait, le prix des serveurs, des licences et des installations sont multipliés par deux. Des dépenses que la plupart des entreprises peuvent difficilement s'autoriser aujourd'hui.

Recourir aux technologies de virtualisation

Mais ce n'est parce que les bandes de stockage s'avèrent peu pratiques et le mirroring trop onéreux que les entreprises doivent faire une croix sur une bonne stratégie de reprise sur sinistre. Heureusement, d'autres solutions existent, qui comblent l'écart entre ces deux approches. Les entreprises qui savent anticiper font ainsi abondamment usage de la virtualisation des serveurs, et pas uniquement pour consolider des machines physiques sur des hôtes virtuels. Certes, les technologies de virtualisation comme vSphere de VMware et Hyper-V de Microsoft, ou les solutions open source Xen et KVM ont d'abord été utilisées pour consolider des serveurs physiques avec, à la clé, de nombreux avantages tels que la réduction du coût des serveurs, la baisse de la consommation d'énergie et la libération d'espace dans les centres de données. Mais il faut savoir qu'il est également possible de recourir à ces technologies dans le cadre d'une stratégie complète de reprise sur sinistre, dans le but de protéger les informations et les systèmes essentiels à la bonne marche des entreprises.

(1) *Cette journée, organisée par l'ONU, s'est tenue le 13 octobre 2013 (http://www.un.org/fr/events/disasterreductionday/).*