SESSION 2015

BREVET DE TECHNICIEN SUPÉRIEUR

ASSISTANT DE GESTION DE PME PMI

À RÉFÉRENTIEL COMMUN EUROPÉEN

Analyse du système d'information et des risques informatiques

Coefficient : 2
Durée : 2 heures

AUCUN MATÉRIEL ET DOCUMENT AUTORISÉS

Dès que le sujet vous est remis, assurez-vous qu'il est complet.
Le sujet comporte 15 pages numérotées de 1 à 15 dont une à rendre avec la copie (annexe A).

AVERTISSEMENT

Dans le souci du respect de la propriété intellectuelle et du droit d'auteur, les extraits d'articles de presse spécialisés ou non, sont reproduits en leur état originel. Ils sont donc susceptibles de comporter des mots ou expressions de style oral ou professionnel.

COMPOSITION DU CAS

Partie 1 : GESTION DE L'INFORMATION

A) Amélioration du processus de commande par internet

B) Préparation de la négociation des achats d'électroménagers

Partie 2 : PARTICIPATION À LA GESTION DES RISQUES INFORMATIQUES

A) Installation du réseau informatique de l'agence de Mâcon

B) Prévention des risques informatiques

Annexes à consulter :

Annexe 1 : Demande de prix sur le site internet

Annexe 2 : Processus de commande, entretien avec M.Neveu

Annexe 3 : Extrait du schéma relationnel de la base de données des commandes

Annexe 4 : Requête demandée par le gérant

Annexe 5 : Informations sur l'installation réseau de la nouvelle agence de Mâcon

Annexe 6 : Schéma du réseau informatique de l'agence de Mâcon

Annexe 7 : Incidents informatiques survenus depuis 2012

Annexe 8 : Recommandations de sécurité relatives aux terminaux mobiles

Annexe 9 : Lexique SQL

Annexes à compléter et à rendre avec la copie :

Annexe A : Processus d'achat d'appareils électroménagers pour MTVE

RECOMMANDATIONS IMPORTANTES

Chaque partie doit être traitée d'une manière indépendante. Cependant, la candidate ou le candidat ne doit pas négliger l'ordre dans lequel les parties sont présentées. Le respect de cet ordre permet de mieux s'imprégner du sujet. La candidate ou le candidat devra en outre faire preuve de discernement afin de repérer dans les documents annexes l'essentiel de l'accessoire.

Enfin, il est rappelé à la candidate ou au candidat que son nom ne doit pas apparaitre dans la copie. En l'absence de précision dans le sujet, l'assistant(e) de gestion de PME/PMI sera madame ou monsieur X.

BARÈME INDICATIF

Partie 1 : 24 points

Partie 2 : 16 points

Présentation du contexte

La société G.S.E (groupement des sociétés électriques) est une entreprise spécialisée dans les travaux d'installation, de maintenance et de dépannage électrique et domotique. Elle a été créée en 1994 par Monsieur Christian Neveu puis s'est développée rapidement par la création d'agences spécialisées. Elle regroupe désormais 55 personnes réparties sur les différentes agences.

Elle est située à Saint-Denis-les-Bourg (département de l'Ain) et compte près de 6 000 clients dans le département de l'Ain mais également à Lyon, à Paris et en Suisse. Ses clients sont pour l'essentiel composés de professionnels (80 %). Les appels d'offres passés avec les acteurs des marchés publics représentent 40 % de son chiffre d'affaires. La société G.S.E. reçoit au siège les demandes des clients puis répartit les tâches dans les agences respectives.

Elle comprend quatre agences opérationnelles dans le département de l'Ain :

- **Neveu Maintenance** propose son savoir-faire et ses nombreuses années d'expérience aux particuliers du département de l'Ain, dans les domaines maintenance et dépannage électrique à domicile, entretien d'équipements électriques, installation de systèmes de réception terrestre et satellite, domotique (automatisation de domiciles) et dépannage d'urgence 24h/24 et 7j/7 grâce à un service d'astreinte ;
- **Neveu Electricité Générale** est spécialisée dans la réalisation de chantiers électriques de grande envergure dans le département de l'Ain et ses environs ;
- **ACTEM Industrie** est spécialisée dans l'assemblage et le montage de tableaux électriques et de systèmes électriques dans le département de l'Ain ;
- **MTVE (Marboz TéleVision Electroménager)** est spécialisée dans la vente et la maintenance d'appareils électroménagers aux particuliers et aux fournisseurs de cuisine.

La société GSE connait actuellement un développement important :

- une agence située à Mâcon va ouvrir ses portes avant la fin de l'année 2015, elle sera gérée par monsieur Perrichoud qui est chargé de son démarrage.

- un site *web* a été mis en place pour développer les ventes d'appareils électroménagers.

Monsieur Neveu, gérant de la société G.S.E., vient de vous engager en qualité d'assistant(e) de Gestion. Votre mission consiste à intervenir auprès des responsables de l'agence MTVE et de la nouvelle agence de Mâcon.

Partie 1 : Gestion de l'information (annexes 1 à 4, annexe 9 et annexe A)

La société MTVE (Marboz TéléVision Electroménager), créée en 2000, a été mise en place afin de fournir une activité complémentaire au groupe. Cette entité est gérée par un gérant, un commercial et un technicien qui intervient sur site. Les clients ont la possibilité d'effectuer leurs achats sur le point de vente de Marboz ou par le biais du site *web* « Neveu Electricité ».

L'**annexe 1** propose une copie d'écran du bon de commande à compléter sur le site. L'**annexe 2** présente un entretien avec M. Neveu pour comprendre le fonctionnement du processus actuel des achats par internet. **L'annexe A** est une ébauche de schématisation du processus.

A) Amélioration du processus de commandes par internet

M. Neveu a décidé de faire évoluer son site *web* car le processus de commande actuel n'est pas très performant. De nombreuses consultations ne sont pas transformées en commande.

Vous êtes chargé(e) de :	
1.1	Identifier les dysfonctionnements actuels liés à la recherche de disponibilités via le formulaire du site *web* de l'entreprise **(annexes 1 et 2).**
1.2	Compléter le diagramme évènement-résultat du processus de commande **(annexe A)** à partir du moment où le client accepte le devis d'après les informations fournies en **annexe 2**.
1.3	Déterminer les obligations du responsable du site en matière de droit à l'information dans le cadre de la collecte et du traitement des données nominatives.

B) Préparation de la négociation des achats d'électroménagers

Le contrat de partenariat avec la centrale d'achat COPRA arrive à son terme et doit être renégocié. C'est M. Neveu qui se charge de négocier tous les achats pour le groupe. Afin de préparer sa négociation, il souhaite que le gérant de MTVE lui fournisse des indicateurs quantitatifs de vente par marque et par type de clients (particuliers ou professionnels) à partir de la base de données de l'entreprise.

L'**annexe 3** présente le schéma relationnel de la base de données de l'entreprise MTVE. L'**annexe 4** présente le résultat de la requête demandée par le gérant. Vous disposez d'un lexique SQL en **annexe 9**.

Vous êtes chargé(e) de :	
1.4	Réaliser une requête permettant à M. Neveu d'avoir un état des produits (code du produit, désignation du produit, marque du produit et prix du produit) classés du plus cher au moins cher pour pouvoir négocier les prix.
1.5	Réaliser la requête en langage SQL qui permet d'obtenir le montant des commandes (quantités commandées totales x prix de vente HT) réalisé par marque pour la période du 1er janvier 2014 au 31 décembre 2014 **(conformément à la demande esquissée en annexe 4)**.

Monsieur Neveu prévoit de faire des remises de :

- 10 % aux grossistes,
- 5 % aux artisans,
- 2 % aux particuliers.

Vous êtes chargé(e) de :	
1.6	Indiquer sur votre copie les modifications à apporter au schéma relationnel pour prendre en compte cette demande (ne faire apparaitre que les relations modifiées ou ajoutées).

Partie 2 : Participation à la gestion des risques informatiques (annexes 5 à 8)

A) Installation du réseau informatique de l'agence de Mâcon

L'agence de Mâcon constitue une nouvelle entité du groupe Neveu spécialisée dans la vente de produits électroniques aux industriels. Monsieur Perrichoud en assurera la gérance en qualité de directeur. L'agence comprend huit personnes qui doivent avoir un accès régulier aux postes informatiques. Pour l'instant six postes informatiques sont connectés au réseau dont un ordinateur portable ainsi que deux imprimantes, une à impression noir et blanc et l'autre à impression couleur. Monsieur Perrichoud souhaite connecter le plus rapidement possible deux stations supplémentaires.

L'annexe 5 présente des informations fournies par le directeur de la nouvelle agence de Mâcon concernant le réseau de cette agence.

L'annexe 6 présente le schéma du réseau de l'agence de Mâcon.

Monsieur Neveu vous demande de proposer un adressage IP (Internet Protocol) complet des nouveaux hôtes du réseau de la nouvelle agence en utilisant des adresses IP fixes. Ce travail doit permettre de réaliser le paramétrage pour chaque matériel pour sa connexion au réseau local et à internet. Par ailleurs, dans la perspective d'un développement du parc informatique, il serait souhaitable d'envisager d'attribuer ultérieurement des adresses IP de façon automatique.

Vous êtes chargé(e) de :	
2.1	Proposer un paramétrage complet à mettre en place sur le poste de travail permettant aux deux nouvelles stations de se connecter au réseau local et au réseau *web* **(annexe 5 et annexe 6).**
2.2	Présenter une solution permettant d'obtenir une adresse IP automatiquement lors de la connexion d'un nouveau matériel sur le réseau.

B/ Prévention des risques informatiques

Monsieur Neveu a recensé les incidents liés à l'utilisation du système informatique. Il a par ailleurs constaté que le logiciel antivirus utilisé actuellement ne donnait pas entièrement satisfaction.

Il s'occupe personnellement des sauvegardes des données du siège de Saint-Denis-Les-Bourg. Une sauvegarde incrémentielle démarre automatiquement tous les soirs à 22 h. Elle concerne l'ensemble des données installées sur les serveurs du siège.

Enfin, le directeur constate, depuis quelque temps, que plusieurs salariés apportent leur travail à la maison mais que des éléments de vie personnelle viennent aussi au travail (via les réseaux sociaux notamment).

Ce phénomène s'illustre également dans les pratiques de BYOD (*Bring Your Own Device*), qui consistent à utiliser les appareils personnels (*smartphones*, tablettes, etc.) dans un cadre professionnel, afin de gagner en flexibilité et en confort. Monsieur Neveu vous interroge donc sur les risques potentiels pour l'entreprise face à cette nouvelle tendance.

L'annexe 7 présente les incidents informatiques survenus depuis 2012. **L'annexe 8** présente les recommandations relatives à la sécurité des terminaux mobiles.

Vous êtes chargé(e) de :	
2.3	Suggérer une solution à M. Neveu pour prévenir et traiter chaque problème rencontré. Vous présenterez votre travail sous la forme d'un tableau **(annexe 7)**.
2.4	En vous appuyant sur **l'annexe 8** et sur vos connaissances, vous présenterez, dans une note structurée, les risques liés à la pratique du BYOD ainsi que les solutions à mettre en place pour limiter ces risques.

Annexe 1 : Demande de prix sur le site internet

Demande de prix

Vous souhaitez faire une demande de prix ?

Remplissez le formulaire ci-dessous, nous vous répondrons le plus rapidement possible.

Vos coordonnées

Votre nom

Votre email

Votre numéro de téléphone

Adresse

Ville | Code Postal

Message

Quantité demandée : 1

Conformément à la loi "informatique et libertés" du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à M. NEVEU, 71 rue de la Tour, 01000 SAINT DENIS LES BOURG

Annexe 2 : Processus de commande, entretien avec M. NEVEU

- **Comment les clients peuvent-ils faire une demande de prix ?**

Nous proposons actuellement au client de faire une demande de prix sur notre site *web*. Toutefois, comme le catalogue n'est pas encore en ligne, le client doit, dans son message, nous indiquer précisément le nom du produit souhaité.

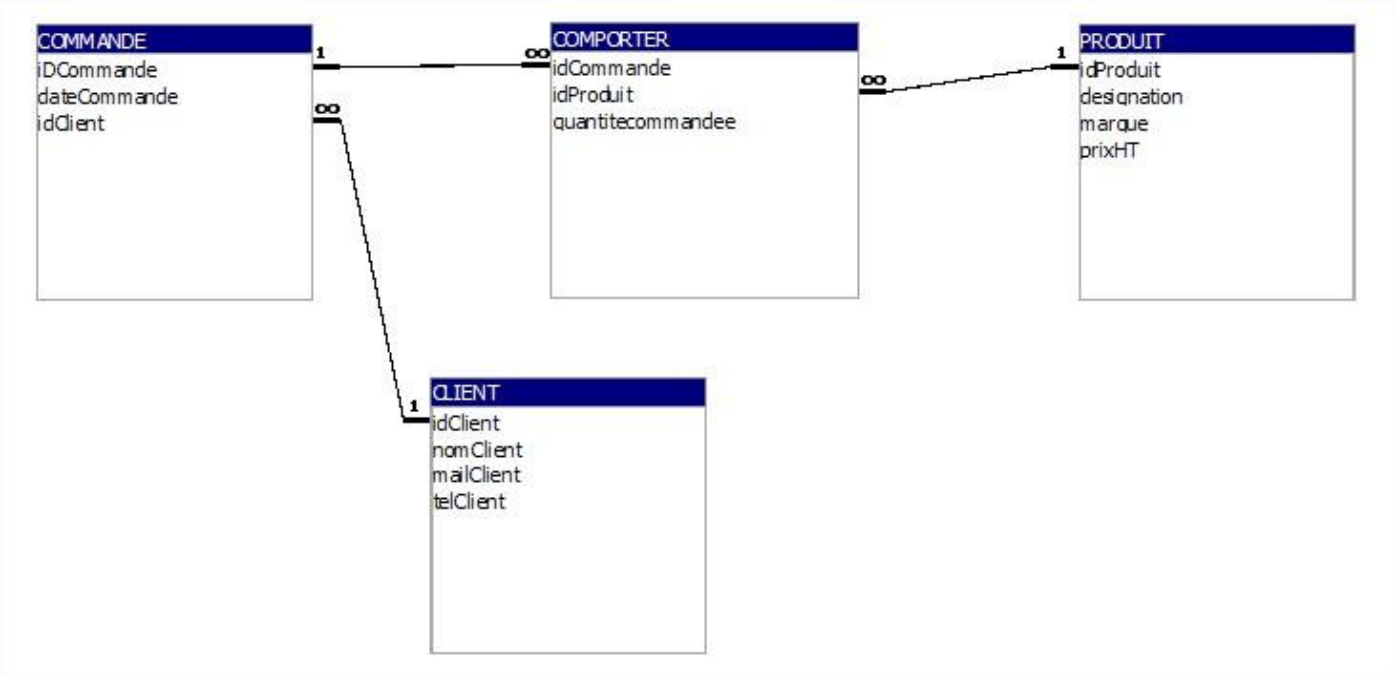
- **Comment cette demande de prix est-elle traitée ?**

La demande de prix est envoyée à une adresse courriel dédiée et gérée par le magasin de l'agence MTVE. À la réception de la demande de prix, le commercial vérifie si MTVE propose ce produit et cette référence. Il consulte ensuite les disponibilités sur la base de données COPRA de la centrale d'achat de notre fournisseur. En fonction des disponibilités, il répond au client positivement ou il l'invite réaliser une nouvelle demande de prix pour un nouveau produit. L'échange de messages et le temps de réponse pour trouver un produit disponible, qui correspond à la demande du client, peut parfois prendre du temps et décourage souvent le client.
Si la demande de prix peut être honorée, le commercial émet un devis à partir du PGI Winbat et le génère en PDF pour être envoyé par courriel au client.

- **Quand démarre le processus de commande ?**

Une fois le devis accepté, le commercial procède à la commande auprès de la centrale d'achat (saisie puis envoi de la commande par fax). Une fois le produit reçu, accompagné du bon de livraison fournisseur, et vérifié par le commercial dans nos locaux, il édite le bon de livraison client pour le technicien et la facture pour validation par le gérant. Le technicien livre et installe le produit chez le client et lui remet le bon de livraison. Le gérant valide la facture, l'envoie au client et classe le double dans le dossier client.

Annexe 3 : Extrait du schéma relationnel de la base de données des commandes

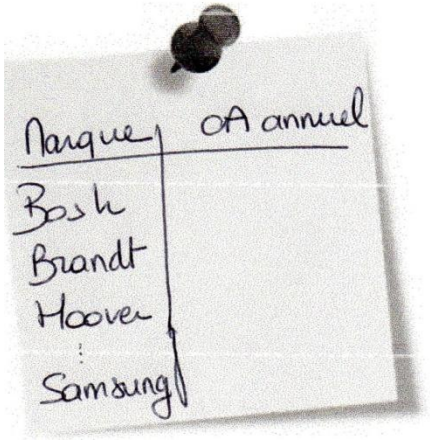


Légende :

1 ——————∞ lien entre clé primaire et clé étrangère

Annexe 4 : Requête demandée par le gérant

Le gérant a laissé un post-it présentant le résultat de la requête qu'il souhaite obtenir pour le chiffre d'affaires (quantités commandées totales x prix de vente HT) réalisé par marque pour la période du 1er janvier 2014 au 31 décembre 2014.

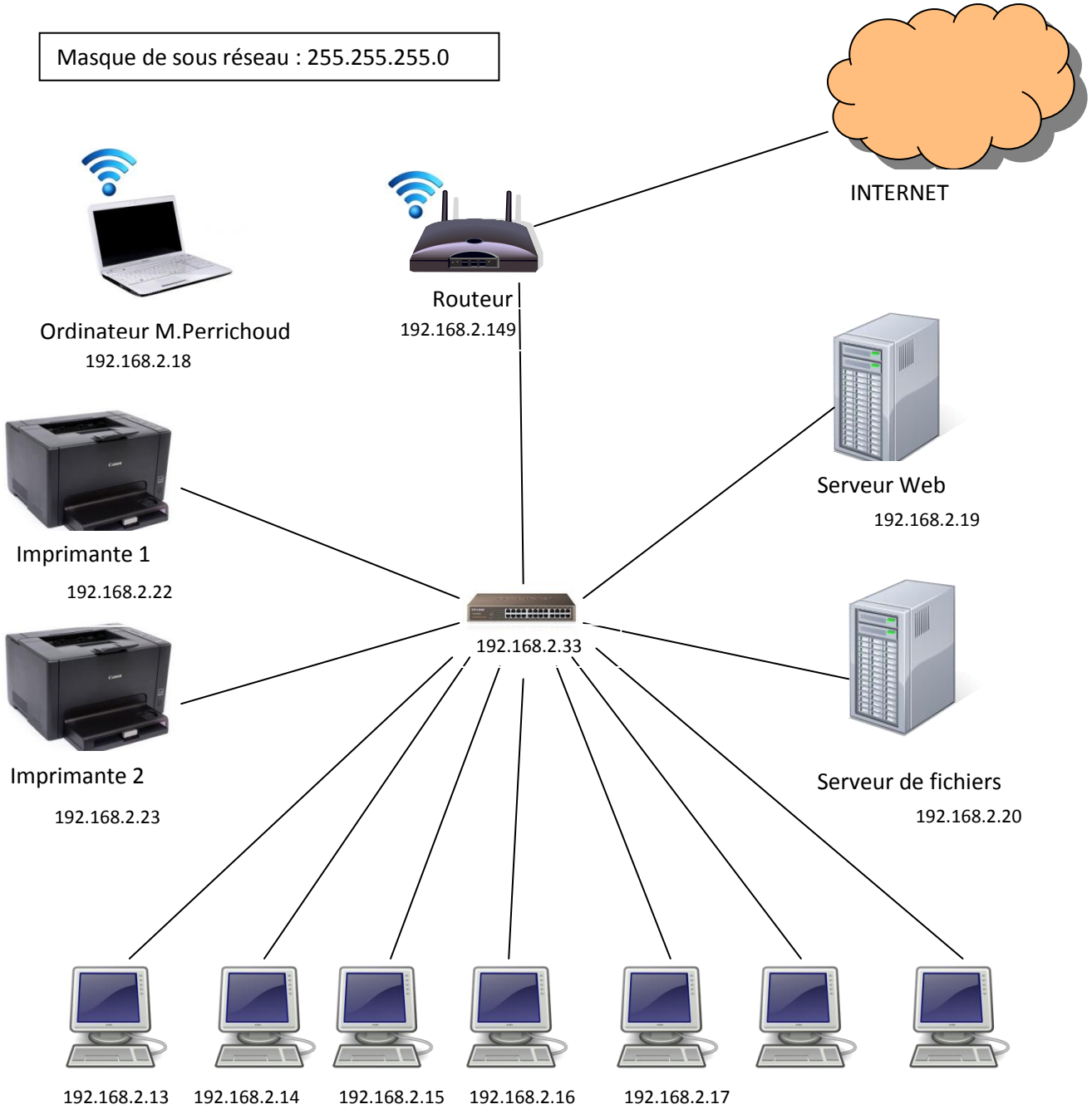


Annexe 5 : Informations sur l'installation réseau de la nouvelle agence de Mâcon

Informations recueillies par l'assistant (e) de gestion auprès de monsieur Perrichoud, directeur d'agence, concernant l'équipement de l'agence de Mâcon :

- Les imprimantes sont accessibles à tous les membres du personnel y compris au directeur.
- Le réseau comprend un serveur utilisé pour gérer les applications propres à l'activité de l'agence de Mâcon. L'application PGI (progiciel de gestion intégré) est installée sur un serveur, les autres agences utilisent cette application via un navigateur *web*.
- Un routeur permet un accès à internet via une connexion ADSL.
- Pour l'instant, nous utilisons des IP fixes pour l'ensemble de nos hôtes intégrés sur le réseau. Il faut prévoir une solution qui nous permettra d'attribuer une adresse IP automatiquement pour chaque matériel nouveau installé sur le réseau.
- Le réseau doit à terme être sécurisé contre les agressions extérieures.
- Les serveurs sont installés dans une pièce séparée des bureaux dans lesquels travaillent les collaborateurs.
- Des surtensions électriques apparaissent quelquefois. Elles sont susceptibles d'endommager les matériels informatiques. Il conviendra d'envisager une solution permettant d'éviter les problèmes électriques.
- Le poste du directeur est doté d'une connexion WiFi.

Annexe 6 : Schéma du réseau informatique de l'agence de Mâcon



Stations des collaborateurs

Annexe 7 : Incidents informatiques survenus depuis 2012

N°	Date	Problème constaté
1	24/07/2012	Problème de mise à jour automatique de l'antivirus. La mise à jour s'établit manuellement toutes les deux semaines depuis ce jour.
2	03/08/2012	Température de 38°C relevée dans le local réseau, arrêt temporaire du serveur. Redémarrage le 06/08/2012.
3	18/03/2013	Deux collaborateurs utilisent le même identifiant à la suite de la perte d'un mot de passe réseau par l'un d'entre eux (les mots de passe qu'ils ont créés librement contiennent 4 caractères).
4	25/07/2013	Suite à un violent orage, une carte réseau défectueuse et une alimentation d'un poste ont été changées.
5	24/03/2014	Un disque du serveur est hors service, la saisie des journées du 20/03/2014 et 21/03/2014 est à reprendre, une copie de sauvegarde avait été réalisée le 19/03/2014.
6	02/04/2014	Courriel reçu de notre banque visant à fournir nos références bancaires pour vérification. La banque a été contactée mais n'est pas à l'origine de cette demande.

Annexe 8 : Recommandations de sécurité relatives aux terminaux mobiles

1. Préambule

L'usage des ordiphones (*smartphones*) ou des tablettes est de plus en plus répandu en environnement professionnel.

Ces terminaux permettent par exemple, en plus d'être joignable, de consulter ses courriels et de naviguer sur internet à la recherche de tout type d'information. Plus encore, ils rendent possible la connexion à un réseau d'entreprise pour travailler sur des applications métier ou accéder à des documents comme tout un chacun le ferait depuis son poste de travail professionnel. En parallèle, de nombreux usages personnels, souvent ludiques, de ces appareils sont entrés dans les mœurs.

On observe une volonté des utilisateurs de pouvoir bénéficier de toutes ces fonctionnalités, dans la sphère privée comme dans la sphère professionnelle, ce qui se traduit par une demande accrue auprès des directions de systèmes d'information de déployer les moyens nécessaires. Leur usage est toutefois problématique. En effet, les solutions de sécurisation actuelles sont peu efficaces pour assurer une protection correcte des données professionnelles. […]

2. Les terminaux mobiles : quels risques de sécurité ?

Les terminaux mobiles stockent des données qui sont enregistrées volontairement (courriels, agenda, contacts, photos, documents, SMS, etc.) ou involontairement (cache de navigation, historique de déplacements datés et géo-localisés, etc.) […]

En particulier, la tendance inopportune des utilisateurs à utiliser des mots de passe identiques pour accéder à plusieurs services différents laisse craindre que les mots de passes stockés dans un ordiphone correspondent potentiellement à ceux de services sensibles. Pèsent alors des risques de modification, de destruction ou encore de divulgation de données professionnelles. […]

Il convient de le prendre en compte sérieusement dans un contexte professionnel. Un attaquant pourra par exemple chercher à pénétrer le système d'information d'une organisation en utilisant comme point d'entrée un terminal mobile. Cela est dû principalement à la multitude de vulnérabilités que présentent les systèmes d'exploitation mobiles mais aussi aux erreurs de comportement d'utilisateurs non avertis.

3. Recommandations de sécurité […]

3.1 Contrôle d'accès […]

Il convient d'analyser, en fonction de la technologie du terminal, la robustesse des mécanismes de verrouillage offerts. On notera que le déverrouillage par symbole (points à relier) ne dispose pas d'une richesse combinatoire suffisante pour être conforme au niveau minimal recommandé. […]

3.2 Sécurité des applications

Interdire l'utilisation du magasin d'applications par défaut, ainsi que l'installation d'applications non explicitement autorisées par l'entreprise. Cette recommandation vaut également pour les applications pré-installées. […]

3.3 Sécurité des données et des communications […]

Désactiver systématiquement l'association automatique aux points d'accès WiFi configurés dans le terminal afin de garder le contrôle sur l'activation de la connexion sans-fil. […]

Tout échange d'informations sensibles doit se faire par un canal chiffré de manière à assurer confidentialité et intégrité des données de point à point.

Note : L'utilisation de solutions VPN dédiées de préférence qualifiées par l'agence peut s'avérer nécessaire pour pallier l'absence native de chiffrement ou un chiffrement peu robuste. […]

4. Cohabitation des usages privés et professionnels

Du fait des recommandations précédentes, la cohabitation des usages privés et professionnels sur un même terminal doit être étudiée avec attention. Dans la plupart des cas, le terminal professionnel devra être dédié à cet usage (l'utilisateur pouvant généralement utiliser son propre terminal pour les usages personnels).

Si l'utilisation d'un seul ordiphone pour les deux contextes ne peut pas être évité, selon la sensibilité des données de l'entreprise traitées sur le mobile, il convient de mettre en œuvre des solutions dédiées pour cloisonner efficacement chaque environnement (personnel, professionnel) en étant vigilant sur les niveaux de sécurité variés des solutions du marché.[…]

5. Exploitation de failles du système d'exploitation ou d'applications

Les systèmes d'exploitation des terminaux mobiles présentent des vulnérabilités. Ces dernières permettent parfois d'accéder aux couches basses du système et peuvent être utilisées par exemple pour y ajouter des portes dérobées ou des codes d'interception. Ces vulnérabilités sont souvent exploitables par le biais d'applications ou directement à travers les interfaces du terminal (port USB, carte WiFi ou Bluetooth, etc.). Difficilement détectable, la compromission résultante permet à une personne malveillante d'avoir un contrôle total du terminal pour intercepter discrètement toutes les données présentes voire pour activer les caméra et microphone de l'équipement.

Paris, le 19 juin 2013,

ANSSI[1] (agence nationale de la sécurité des systèmes d'information)

[1] Agence placée sous l'autorité du ministère de défense et chargée d'assurer la sécurité informatique de l'État.

Annexe 9 : Lexique SQL

Notation utilisée

- Les éléments entre crochets [ ] sont facultatifs.
- « colonne » désigne le nom d'une colonne éventuellement préfixé par le nom de la table à laquelle elle appartient : « nomTable.nomColonne ».
- « élément1 [, élément2 ...] » signifie une liste d'éléments (noms de colonne par exemple) séparés par une virgule. Cette liste comporte au minimum un élément.

Ordre SELECT

SELECT [DISTINCT] colonne1 [AS nomAlias1] [, colonne2 [AS nomAlias2] …]

FROM nomTable1 [nomAlias1] [, nomTable2 [nomAlias2] …]

[WHERE conditionDeRestriction**]**

[ORDER BY colonne1 [DESC] [, colonne2 [DESC] …] **]**

- La liste de colonnes située après le mot SELECT peut être remplacée par le symbole "".*

Condition de restriction (ou de sélection)

Une condition de restriction (désignée dans ce mémento par « conditionDeRestriction ») peut être composée d'une ou de plusieurs conditions élémentaires combinées à l'aide des opérateurs logiques NOT, AND et OR, en utilisant éventuellement des parenthèses.

Conditions élémentaires	
colonne = valeurOuColonne	colonne <> valeurOuColonne
colonne < valeurOuColonne	colonne > valeurOuColonne
colonne <= valeurOuColonne	colonne >= valeurOuColonne
colonne IS [NOT] NULL	colonne LIKE filtre
colonne BETWEEN valeur1 AND valeur2	colonne IN (valeur1, valeur2, …)

- "filtre" désigne une chaîne de caractères comportant les symboles "%"et/ou "_".

- Les filtres peuvent être utilisés avec une colonne de type chaîne ou date.

- Certains SGDB utilisent "" et "?" au lieu de "%" et "_" pour l'écriture des filtres.*

Regroupement de lignes

SELECT [colonne [,..., colonne]] [, COUNT(*)] [SUM(Colonne)] [AVG(colonne)]

FROM table [, …, table]

[**WHERE** condition

GROUP BY colonne [,…., colonne]

[HAVING condition]

Annexe A : Processus d'achat d'appareils électroménagers pour MTVE

Annexe à compléter et à rendre avec la copie