RAPPORT DE PRECONISATIONS : EQUIPE ANALYSE

Réalisé par :

Alcaraz Jeremy
Bastien Remi
Chane-To Sébastien
Daunis Nicolas
Gouret Mathieu
Laraki Ilham
Le Louarn Pierre-Yves
Leroux Gillian
Mechhour Youssef
Milano Yannick
Mouron Sébastien
Tinelli Vincent
Vivier Yoann
Valentie Remy

Master 2 STRI Université Paul Sabatier 2009/2010

Table des matières

I. Introduction

Depuis de nombreuses années, les dépenses en matière de sécurité ont considérablement augmentés dans certains secteurs industriels. C'est devenu une préoccupation et un pôle majeur jusqu'à obtenir le statut de haute priorité pour certain dirigeants. La Sécurité des Systèmes Informatiques est de plus en plus un point central, non seulement pour l'investissement, mais aussi doit être un retour sur cet investissement.
Dans le cadre du projet linux « Attaque – Défense – Audit » la question des méthodes d'audits portant sur la Sécurité des Systèmes Informatiques est, comme nous venons de le voir, une part non négligeable du contexte dans le quelle nous évoluons. Avant d'élaborer une politique SSI, basée sur le résultat d'un audit, il semble nécessaire de bien préciser, de définir de quoi elle est composée et à quoi elle sert

1. Définition de la Politique SSI

1 : Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.

2 : La politique SSI constitue ainsi le socle de la SSI. C'est le référentiel qui "fait foi", théoriquement à tout moment, au sein du périmètre dans lequel il s'applique. Toute réflexion relative à la SSI dans le cadre de ce périmètre devra être conforme à cette politique.

3 : La politique SSI traduit la reconnaissance officielle de l'importance accordée par la direction de l'organisme à la sécurité de son système d'information.

Elle doit donc mettre en évidence le socle de toute réflexion relative à la SSI :

- le périmètre de la politique SSI décrit son champ d'application,
- les enjeux illustrent l'importance du périmètre et les buts à atteindre,
- les références applicables recensent les normes à respecter,
- les grands besoins de sécurité mettent en évidence ce que l'organisme veut protéger ; ils sont généralement exprimés en termes de disponibilité, d'intégrité et de confidentialité,
- les grandes menaces décrivent les événements redoutés et leur origine.

4 : Une politique SSI doit refléter la prise en compte de :

- toutes les ressources,
- tous les acteurs,
- l'ensemble du cycle de vie des systèmes d'information,
- toutes les possibilités pour traiter des risques.

Voici un exemple de structuration des règles de sécurité de l'ISO 27002 :

- politique de sécurité,
- organisation de la sécurité de l'information,
- gestion des biens,
- sécurité des ressources humaines,
- sécurité physique et environnementale,
- gestion des communications et opérations,
- contrôle d'accès,
- acquisition, développement et maintenance des systèmes d'information,
- gestion des incidents de sécurité de l'information,
- gestion de la continuité d'activités,
- conformité.

En d'autre terme une politique SSI doit comprendre des règles de sécurité, plus ou moins détaillées, mais qui traitent de tous les thèmes de la SSI, et qui devront être appliquées.

2. Présentation de méthodes d'audit et normes

Il existe de nombreuses méthodes permettant de réaliser des audits des Sécurité des Systèmes Informatiques aboutissant à une politique des SSI.

Ci-dessous les principales méthodes d'audit

Méthode	Création	Popularité	Auteur	Soutenue par	Pays	Outils disponibles	Etat
EBIOS	1995	***	DCSSI	gouvernement	France	logiciel gratuit	
Melisa		**	DGA	armement	France		abandonnée
Marion	1980	**	CLUSIF	association	France		abandonnée
Mehari	1995	***	CLUSIF	association	France	logiciel Risicare	
Octave	1999	**	Université de Carnegie Mellon	universitaire	Etats-Unis	logiciel payant	
Cramm	1986	**	Siemens	gouvernement	Angleterre	logiciel payant	
SPRINT	1995	*	ISF	association	Angleterre	logiciel payant	
BS 7799		***		gouvernement	Angleterre		
ISO 17799		***		international			
ISO 13335				international			
ISO 15408				international			
SCORE	2004		Ageris Consulting	secteur privé	France	logiciel payant	
CALLIO	2001		CALLIO Technologies	secteur privé	Canada	logiciel payant	
COBRA	2001		C & A Systems Security Limited	secteur privé	Angleterre	logiciel payant	
ISAMM	2002		Evosec	secteur privé	Belgique		
RA2	2000		aexis	secteur privé	Allemagne	logiciel payant	

II. Constat sur CANDIDE SA

Rappel des faits

Voici les constatations que notre société à pu faire sur l'entreprise CANDIDE SA :

- La fuite d'information :

Le lundi 09/10/09, un membre de CandideSA a perdu des informations sensibles. Il s'agissait d'un des administrateurs du parc de l'entreprise. Il a perdu les backups des serveurs, le mot de passe de la passerelle de l'entreprise (VPN, routage et filtrage), son accès personnel à l'espace collaboratif et au webmail.
Ces données ont rapidement été rendues publiques, forçant CandideSA à couper tous ses services pour éviter que ses concurrents ne viennent capturer les données confidentielles.

- Les réactions :

Aucun responsable de CandideSA n'a pris la peine de communiquer sur la fuite d'informations, sur son ampleur et sur la politique qui allait être mise en œuvre. Les clients n'ont pas été contactés non plus.

- Les périphériques

L'entreprise CandideSA n'a pas envisagé la sécurisation physique de son parc de machines. En effet, nous sommes arrivés à nous introduire dans l'architecture de CANDIDE SA à l'aide de clavier KEYLOGGER.
Comme nous l'avons déjà dit dans des précédents rapports, les utilisateurs n'ont pas été sensibilisés sur les problèmes d'utilisation de machine non contrôlé par l'entreprise. (Les machines dont l'accès n'est pas vérifié ou vérifiable)
Par conséquent, le matériel a pu rester en place pendant 3 semaines, et même après la fuite de données simulée les comportements n'ont pas évolué, puisque les mots de passe ont pu être enregistrés par nos claviers.
Les premières informations intéressantes sont apparues rapidement :

- ✓ Passphrase de chiffrement des disques dur ;
- ✓ Mot de passe root des serveurs et du routeur FreeBSD ;
- ✓ Identifiant du wiki d'un utilisateur, pour lequel il manquait le code à 3 chiffres saisi à la souris ;
- ✓ Différents identifiants de webmail et autres sites de nombreux utilisateurs.

- Les mots de passe :

A l'heure actuelle, les mots de passe sont acteurs très important en ce qui concerne la sécurité des systèmes d'informations. Il s'est avéré que CANDIDE SA a des lacunes dans ce domaine.

- Le wifi :

La société CANDIDE SA dispose de point d'accès WIFI qui furent piraté lors de la troisième attaque. En effet la politique de chiffrement choisi n'était pas suffisante pour permettre à l'entreprise d'avoir une bonne sécurité.

- Les postes de travail :

Durant la période d'audit, nous avons vu que plusieurs failles aux niveaux logiciels furent exploités telles que par exemple la faille Wordpress.

BILAN

Les constatations que nous venons d'exposer montrent que la société CANDIDE SA dispose de faille de sécurité et nous permettent donc de pouvoir émettre des préconisations à la société CANDIDE SA.

III. Méthode Ebios

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) à été choisi dans le cadre de l'étude du fait d'un grand nombre de document et d'un logiciel d'aide a la mise en forme (gratuite) nous permettant de mener à bien la définition d'une politique de la SSI de la société Candide SA.

1. Présentation

La méthode EBIOS a été crée dans le but de permettre d'identifier les risques relatif à la SSI et de proposer ainsi une politique de sécurité adaptée aux besoins de l'entreprise (ou d'une administration). Elle permet aussi de communiquer à leur sujet au sein de l'entreprise et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI. Elle a été créée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), du Ministère de la Défense (France). Elle est destinée avant tout aux administrations françaises et aux entreprises.

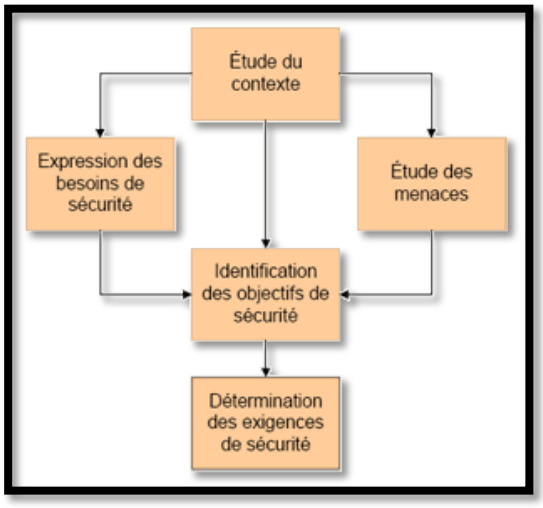
2. Décomposition de la méthode

La méthode EBIOS est composée de 5 guides (Introduction, Démarche, Techniques, Outillages) et d'un logiciel d'aide à la retranscription des différents guides. Elle est compatible avec la norme ISO 17799. La méthode EBIOS est aussi découpée en 5 étapes.

1. Les étapes

Voici les 5 étapes de la méthode EBIOS :

- étude du contexte
- expression des besoins de sécurité
- étude des menaces
- identification des objectifs de sécurité
- détermination des exigences de sécurité



2. *Définition des étapes*

L'étude du contexte permet d'identifier quel système d'information est la cible de l'étude. Cette étape délimite le périmètre de l'étude : présentation de l'entreprise, architecture du système d'information, contraintes techniques et réglementaires, enjeux commerciaux. Mais est aussi étudié le détail des équipements, des logiciels et de l'organisation humaine de l'entreprise.

L'expression des besoins de sécurité permet d'estimer les risques et de définir les critères de risque. Les utilisateurs du SI expriment durant cette étape leurs besoins de sécurité en fonction des impacts qu'ils jugent inacceptables.

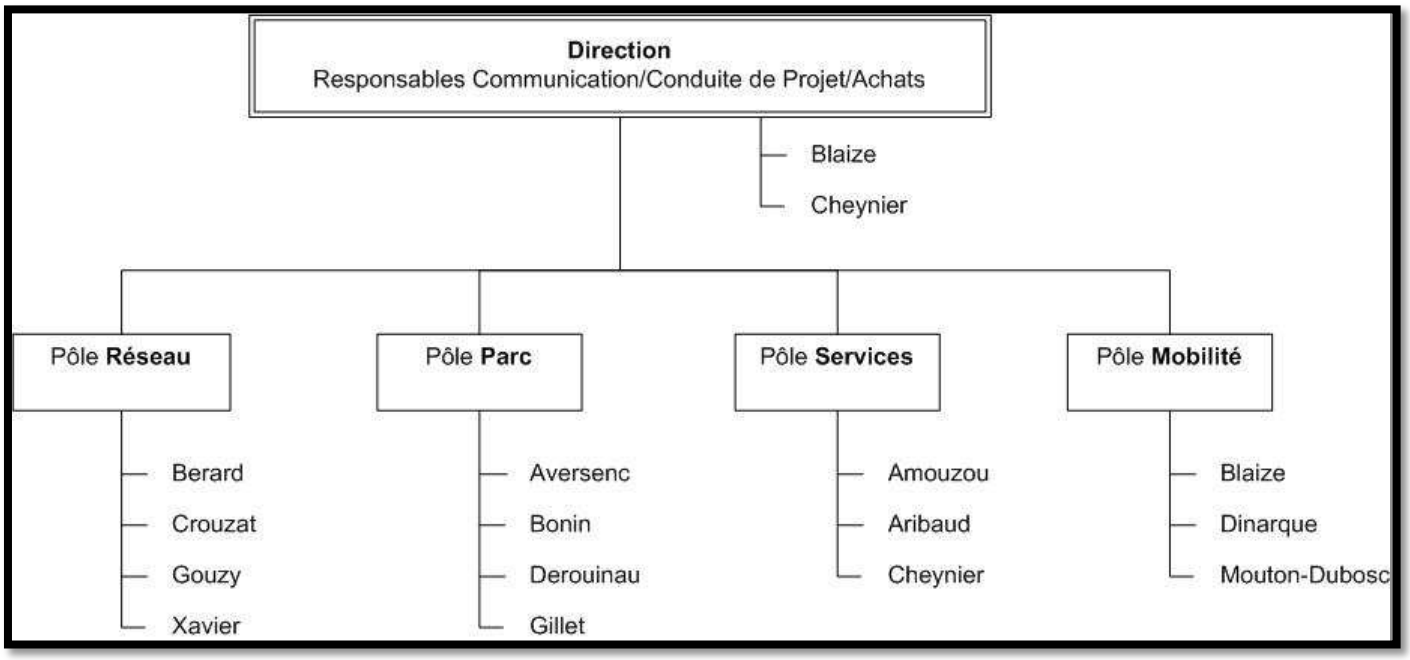
L'étude des menaces permet d'identifier les risques en fonction non plus des besoins des utilisateurs mais en fonction de l'architecture technique du système d'information. Ainsi la liste des vulnérabilités et des types d'attaques est dressée en fonction des matériels, de l'architecture réseau et des logiciels employés. Et ce, quelles que soient leur origine (humaine, matérielle, environnementale) et leur cause (accidentelle, délibérée).

L'identification des objectifs de sécurité confronte les besoins de sécurité exprimés et les menaces identifiées afin de mettre en évidence les risques contre lesquels le SI doit être protégé. Ces objectifs vont former un cahier des charges de sécurité qui traduira le choix fait sur le niveau de résistance aux menaces en fonction des exigences de sécurité.

La détermination des exigences de sécurité permet de déterminer jusqu'où on devra aller dans les exigences de sécurité. Il est évident qu'une entreprise ne peut faire face à tout type de risques, certains doivent être acceptés afin que le coût de la protection ne soit pas exorbitant. C'est notamment la stratégie de gestion du risque tel que cela est défini dans un plan de risque qui sera déterminé ici : accepter, réduire ou refuser un risque. Cette stratégie est décidée en fonction du coût des conséquences du risque et de sa probabilité de survenue. La justification argumentée de ces exigences donne l'assurance d'une juste évaluation.

IV. Analyse des risques du projet

1. Organisation de la société Candide SA



2. Etude du contexte détermination et classification des processus à l'aide d'EBIOS

Le logiciel EBIOS nous permettant d'intégrer directement les données dans sa base. Un document de synthèse concernant la stratégie de sécurité ainsi qu'une étude complète regroupant stratégie de sécurité, Identification des objectifs de sécurité et détermination des exigences de sécurité EBIOS, sont disponibles ci-dessous.

Note de stratégie de sécurité	Document Microsoft Office Word 97 - 200
Méthode Ebios complète	Document Microsoft Office Word 97 - 200

Ces outil vont nous permettent d'insuffler de nouvelles directives à la société CANDIDE SA pour qu'elle appréhende au mieux l'ensemble des objectifs de remise en conformité et ceux avenir concernant sa politique des SSI.

Dans la littérature un principe est largement accepté, est que la gestion des activités ne peut être gérée que si elles peuvent être mesurées.

Enfin, cette études de sécurité va permettre à l'entreprise CANDIDE SA de mieux répondre à des questions tels que:

Sommes-nous plus en sécurité aujourd'hui que nous l'étions avant?
Sommes-nous suffisamment en sécurité?

Une partie des préconisations faite sous EBIOS, sont traitées dans la suite du document.

V. Préconisations

1. Fuite d'informations :

Rappel

L'entreprise possède un nombre très important d'équipements au sein de ses bâtiments, et parfois à l'extérieur chez des clients, sous-traitants, hébergeurs, réparateurs…
Bien souvent la sécurisation physique de ces équipements n'est pas réalisée de manière complète, car on considère qu'en dehors des serveurs jugés « cruciaux », les autres machines ne représentent pas un réel danger.

Comment éviter l'inévitable ?

- Le gouvernement britannique dans l'embarras

86 % du public en Grande-Bretagne ne fait pas confiance à la sécurité informatique de l'administration, selon notre article de presse (en anglais).
http://www.sophos.com/pressoffice/news/articles/2007/11/local-government.html

- Fuite de données via e-mail

50 % des employés admettent avoir déjà envoyé du courrier électronique au mauvais destinataire, révèle une enquête (en anglais) de Sophos.
http://www.sophos.com/pressoffice/news/articles/2007/11/data-leakage-poll.html

- Manque de formation et de sensibilisation des utilisateurs nomades

Les utilisateurs ne sont pas du domaine informatique et ne se rendent pas compte de l'impact de certaines de leurs actions.

Exemples de fuite

- Depuis janvier 2009, la rédaction de ZATAZ.COM a pu faire corriger près de 120 très graves fuites de données.

- Deux disques durs contenant des informations personnelles de 25 millions de britanniques ont été perdus lors d'un transfert postal. Près de la moitié de la population du pays est concernée.

http://www.securityvibes.com/perte-de-donnee-massive-en-grande-bretagne-jsaiz-news-200922.html

- Une clé USB perdue, non chiffrée, est à l'origine de la perte de données personnelles relatives à près de 130 000 détenus et délinquants récidivistes d'Angleterre et du Pays de Galles. Un sous traitant est responsable de la fuite.

http://www.securityvibes.com/angleterre-championne-de-la-perte-de-donnees-elise-news-2001050.html

- Un disque dur perdu par un sous-traitant du ministère anglais de la défénse

http://www.polkaned.net/blog/index.php?post/2008/10/14/148-perte-de-donnees-sensibles-au-uk-la-saga-continue

- Une enquête réalisée par Sky News a mis en avant que des réparateurs d'ordinateurs volaient les données des clients, allant jusqu'à essayer les comptes en banque.

http://news.sky.com/skynews/Home/video/Computer-Repair-Shops-Illegally-Accessing-Personal-Data-From-Customers-Hard-Drives-Sky-News-Investigation/

Vecteurs de fuite

- Courrier électronique (erreur de destinataire)

50% des utilisateurs se sont déjà trompés de destinataire

- Périphériques nomades (Ordinateur portable, Téléphone portable, Clé USB, Disque dur, Cd)

Voir les exemples de l'Angleterre

- Réseaux sociaux

Voir le récent piratage de Twitter : http://www.securityvibes.com/intrusion-social-engineering-twitter-jsaiz-news-3003240.html

- Conversation (Téléphonique, Publique)

Voir les utilisateurs de CandideSA

- Utilisation (Publique, Caméra de surveillance, endroit inaproprié : cybercafé..)

Voir les utilisateurs de CandideSA

- Imprimantes, photocopieurs et poubelles

Se méfier des intervenants extérieurs

CandideSA

L'entreprise CandideSA n'a pas envisagé les fuites de données dans son processus de sécurité. En conséquence, elle n'a pas su communiquer de manière efficace après la fuite.
Et, pour finir elle n'avait pas non plus prévu de mesures de remise en marche rapide de son parc.
Les cas de compromission sont de nos jours relativement rares. Les systèmes déployés sur les serveurs sont par défaut très sécurisés, et à moins de le faire exprès, on est relativement tranquille en se maintenant à jour.
Par contre, la fuite de donnée est inévitable, et n'avoir prévu aucune solution pour réagir dans ce cas est beaucoup plus gênant.
Le downtime de plusieurs jours confirme l'intérêt de prévoir une solution pour réagir rapidement.

Préconisations

En amont pour les utilisateurs

- Former les utilisateurs nomades et les sensibiliser sur les conséquences de leurs actions :
  - ✓ Chiffrement des systèmes de stockage
  - ✓ Identification et utilisation sur des systèmes sécurisés
  - ✓ Se méfier des personnes extérieures
  - ✓ Eviter de travailler en public
  - ✓ Prévenir rapidement les responsables sécurité en cas de doute

- Trop de sécurité tue la sécurité :
  - ✓ Ne pas poser trop de contraintes sur les utilisateurs nomades
  - ✓ Risque de passer outre toutes les recommandations si système trop contraignant

- Fournir aux utilisateurs les fichiers nécessaires uniquement :
  - ✓ Le commercial ne doit pas se déplacer avec un accès complet s'il a besoin de 3 brochures confidentielles

- Nettoyer avant chaque sortie les machines, supports de stockage et téléphones
  - ✓ Clé USB et téléphone à usage unique
  - ✓ Disque dur dans les cas critiques

- Nettoyer après chaque sortie les machines, supports de stockage et téléphones
  - ✓ Un client peut avoir fourni un document vérolé de manière intentionnelle.
  - ✓ Jeter les appareils à usage unique

- Proscrire l'utilisation des postes internes en déplacement :
  - ✓ Masse d'information critique
  - ✓ Possibilité qu'il soit déjà vérolé

En amont pour les administrateurs

- Préparer les fichiers de révocation de certificat à l'avance

- Surveiller son serveur de backup de très prêt :
  - ✓ Isolation physique
  - ✓ Isolation logique (séparation sur le réseau)
  - ✓ Chiffrer les disques, et prévoir le démontage automatique lors du login physique
  - ✓ Désactiver le login distant
  - ✓ Désactiver tous les services superflus
  - ✓ Limiter les intervenants
  - ✓ Ne pas faire confiance à un prestataire
  - ✓ Ne pas l'externaliser n'importe comment

- Prévoir des scripts de réinitialisation et de blacklist des mots de passe et des certificats pour tous les services :
  - ✓ Voir la réaction de Debian, suite au bug sur la génération des certificats
  - ✓ Lister les endroits où sont entreposés les différents certificats

En aval pour les utilisateurs

- Une fois le « coupable » identifié :
  - ✓ Identifier avec lui les erreurs commises, et en informer les collaborateurs pour éviter qu'ils ne la reproduisent
  - ✓ Sensibiliser à nouveau

En aval pour les administrateurs

- Révoquer les certificats compromis

- Identifier le vecteur de fuite ou d'attaque et trouver une solution pour l'éviter ou combler la faille

- Vérifier l'intégrité de tout le parc à l'aide des différents outils disponibles :
  - ✓ Antivirus
  - ✓ Détection de Rootkit
  - ✓ Intégrité matérielle

- En cas de tentative d'intrusion, laisser faire pour voir les données ciblées et identifier les auteurs

- Communiquer sur la fuite de manière publique, prévenir ses clients et collaborateur :

Tout le monde est conscient que cela arrive, autant montrer que l'on sait réagir comme il faut. Plutôt que ne rien dire et que cela sorte de manière incontrôlé sur

2. Poste de travail :

- Respecter la charte d'utilisation des postes de travails (voir annexe 1)
- Installer des antivirus sur les stations clientes et serveurs pour réduire la contamination par des vers.
- Avoir un système pour déployer les mises à jour des postes clients.
- Mettre à jour les logiciels installés.

Exemple : la faille Wordpress

Pour la faille Wordpress, la version était la 2.8.4, une version touchée par une faille. La mise à jour a été proposée 2 jours après la publication de l'exploit. Le cas typique ou se tenir à jour ne suffit pas.

Des choix d'architecture et de configuration auraient pu limiter l'impact :

- ✓ Réglages spécifiques d'Apache et PHP, Cf. resource limits de la configuration PHP :
  - Temps maximal d'exécution
  - Allocation mémoire maximale
  - Taille maximale des paramètres
  - Priorité des processus Apache/PHP : nice/renice
- ✓ Service FTP sur un autre serveur
- ✓ Service mySQL sur un autre serveur

Pour corriger de manière simple et rapide l'attaque du Wordpress nous vous conseillons de modifier ces lignes :

Il faut aller dans wp-trackback.php et trouver la ligne:

```
$charset = $_POST['charset'];
```

et la remplacer par:

```
$charset = str_replace(”,”,””,$_POST['charset']);
if(is_array($charset)) { exit; }
```

Cependant, ce "hack" ne vous protégera que contre cette faille connue désormais, et non pas contre de nouvelles failles de même nature.
Une remise à plat de l'architecture et de la configuration des services seraient souhaitable.

3. Périphériques :

En amont pour les utilisateurs

- Former les utilisateurs et les sensibiliser sur les conséquences de leurs actions :
  - ✓ Identification et utilisation sur des systèmes sécurisés
  - ✓ Ne pas travailler sur une machine externe non contrôlée, mais utiliser son ordinateur portable
  - ✓ Ne pas faire une confiance aveugle aux installations physiques à l'intérieur de l'entreprise.

En amont pour les administrateurs

- Les éléments reliés à l'informatique doivent être pris en compte pour la sécurisation :
  - ✓ Clavier, souris…
  - ✓ Câbles réseaux
  - ✓ Tout périphérique relié à l'ordinateur en général

- Utiliser des matériels « transparents »
  - ✓ Clavier sur lesquelles on peut voir la carte électronique (non opaque)

Générales

- La seule préconisation en aval consiste à prendre en compte les éléments physiques après une compromission, à la place de se focaliser sur les potentielles failles logicielles, il faut aussi vérifier l'intégrité des éléments physiques.

- Le webmail est une source de fuite de mot de passe très important, il faut donc le mettre en place uniquement si nécessaire, et donner l'accès à des utilisateurs sensibilisés. Lorsqu'il est mis en place, un contrôle doit être fait, des mots de passe différents doivent être utilisés, on peut envisager de couper l'accès sur les périodes où l'utilisateur n'est pas en déplacement, changer le mot de passe avant chaque déplacement, et le vider régulièrement des anciens mails.

4. Mot de passes :

- Mettre en place des mots de passe avec un minimum de sécurité pour éviter le piratage. (caractères spéciaux, majuscule, chiffres, lettres, longueur minimum de 8 caractères.)

- Le webmail tant utilisé de nos jours représente un vecteur d'attaque très important, puisque les utilisateurs ont la fâcheuse tendance à laisser leurs identifiants sur des machines publiques. Une fois, l'accès au webmail récupéré, l'attaquant peut facilement récupérer les mots de passe des autres services : Ebay, Paypal, Facebook etc… Il faut donc mettre en place des mots de passes différents pour chaques applications, services, mails…

Exemple des problémes de mot de passes de CANDIDE SA

- Les mots de passe MySQL/PHP en dur: effectivement c'est une contrainte du système, mais utilisé un hash MD5 sur les password est une folie à l'heure actuelle :
  - ✓ Puissance de calcul via GPU ;
  - ✓ http://gdataonline.com/seekhash.php, qui nous a permis de retrouver les mots de passe de l'application Emploi du Temps en très peu de temps. Ils étaient volontairement simples pour laisser une porte à l'attaque, mais le choix de MD5 reste mauvais;
  - ✓ SHA1 voir SHA256 pour les hash en base de données.

- La passphrase de 4 caractères est aussi une erreur pour les raisons suivantes :
  - ✓ facilement crackable(AES128, par défaut juste) ;
  - ✓ entropie très mauvaise;
  - ✓ autant ne pas en mettre pour éviter de pénaliser les performances ;
  - ✓ passphrase = 1 phrase, RTFM;
  - ✓ ne pas se croire en sécurité avec un système chiffré.

- Dump Wiki/Webmail : la sécurité proposée par l'asministration était charmante, il a juste oublié un point (10^3=1000), cela se bruteforce avec wget, 5 lignes de C/Shell à partir du moment ou un inconscient s'est loggé n'importe ou (cas classique en entreprise). Une approche de limitation de login par heure/jour aurait été plus intéressante, avec désactivation du compte au bout de 3 mauvais logins par exemple.

- Les mots de passe administrateurs ne doivent pas être detenus que par une seule personne. En effet comme cela c'est produit lors de la derniére attaque, seul l'administrateur systéme qui était absent ce jour les avaient. Dés lors la réactivité de la société CANDIDE SA fut affaiblie.

5. Wifi :

- Mettre dans un lieu sécurisé d'accés les équipements sensible tel que les bornes WiFi.

- Sensibiliser vos collaborateurs sur le fait de ne pas installer de point d'accès wifi sans l'accord préalable de votre direction informatique. En effet, il suffit qu'un de vos employés branche un point d'accès sur une prise réseau pour que toutes les données de votre réseau wifi soient accessibles à toute personne extérieure pouvant se connecter à une borne wifi.

- Placez votre point d'accès au cœur de l'entreprise, et non pas prêts des fenêtres par exemple ce qui a été fait et permis l'intrusion des attaquants.

- Acquérir plusieurs points d'accès à zone de couverture réduite plutôt qu'un seul à zone de couverture trop importante et pouvant dépasser l'enceinte de l'entreprise.

- Cacher le SSID

- Filtrer les adresses MAC

- Opter pour un chiffrement de type WPA2

- Limiter la puissance d'émission de la borne pour éviter de couvrir une zone trop large.

VI. Bilan

Au travers de ce rapport, nous avons traité la politique de sécurité de l'entreprise CANDIDE SA.

Les constats que nous avons présentés montrent bel et bien que l'entreprise CANDIDE SA dispose de faille de sécurité qu'il est nécessaire de régler pour optimiser la sécurité de l'entreprise.

La méthode EBIOS (expression des besoins et identification des objectifs de sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information.

En fournissant les justifications nécessaires à la prise de décision (descriptions précises, enjeux stratégiques, risques détaillés avec leur impact sur l'organisme, objectifs et exigences de sécurité explicites), EBIOS est un véritable outil de négociation et d'arbitrage.

Les constats ainsi que la méthode EBIOS nous ont donc permis d'émettre des préconisations que notre société peut faire à l'entreprise CANDIDE SA.

Annexe 1 : Chartre d'utilisation des postes de travails

Résumé à l'usage des utilisateurs du Système d'information de CANDIDE SA

La présente note récapitule quelques principes de sécurité à garder à l'esprit dès que l'on allume un ordinateur. Le document joint « Charte d'utilisation des postes de travail de CANDIDE SA » présente le détail des points évoqués ici.

1. Sécurité des mots de passe

Le plus important des articles de cette charte concerne les mots de passe : ils sont strictement personnels, ne doivent pas être trop faciles à deviner, c'est-à-dire qu'ils doivent comporter huit caractères avec des majuscules, des minuscules et des chiffres, et ne doivent sous aucun prétexte être communiqués à un autre que leur possesseur unique. Aucun compte d'utilisation d'un service ou d'un ordinateur ne doit être ouvert sans mot de passe.

2. Distribution des mots de passe

L'application pratique du principe précédent se traduit de la façon suivante : un mot de passe ne doit jamais être écrit sur papier, sauf éventuellement pour une transmission par courrier cacheté à l'adresse personnelle de son utilisateur. Dans ce dernier cas, il devra impérativement être modifié après une première utilisation.

3. Verrouillage des accès

Pour la même raison, qui est d'empêcher l'accès illégitime à des données, un poste de travail dont l'utilisateur s'absente doit être verrouillé de façon à ce que son écran ne soit plus lisible et son clavier inutilisable. Tous les systèmes informatiques permettent facilement ce verrouillage du poste.

4. Compte administrateur

Toujours pour empêcher des corruptions de données ou de logiciel, le compte administrateur des postes de travail ne doit être utilisé qu'à bon escient et par des personnels agréés par le responsable informatique de site. Le travail en routine sous le compte administrateur est une très mauvaise pratique, à prohiber.

5. Respect de la loi Informatiques et Liberté

Bien que cela soit *en principe* superflu, la charte rappelle que les agents de l'Inserm doivent respecter les lois, et notamment la loi Informatique et Libertés ainsi que les lois relatives à la propriété intellectuelle et à la propriété industrielle.

La loi Informatique et libertés protège les personnes contre les abus liés aux fichiers nominatifs. À ce titre, chaque détenteur de fichier nominatif est tenu de prendre toutes les mesures appropriées pour empêcher la divulgation ou l'usage illégitimes de ces données. C'est une responsabilité pénale. Les inspecteurs de la Commission nationale de l'informatique et des libertés (CNIL) sont habilités à infliger des amendes et autres sanctions sans passer par les autorités judiciaires.

6. Utilisation des logiciels

Les logiciels, commerciaux ou libres *(open source)* sont protégés par les lois relatives à la propriété intellectuelle. Leur usage est subordonné au respect d'une licence de droit d'usage, qui, dans le cas des logiciels commerciaux, s'obtient à titre onéreux, par le paiement d'un droit d'usage. Utiliser un tel logiciel sans respecter sa licence de droit d'usage est un délit qui engage la *responsabilité pénale personnelle* de l'agent qui le commet. Les titulaires de droits peuvent faire appel aux autorités judiciaires pour procéder à des saisies-contrefaçon dans les locaux des organismes suspectés de tels usages délictueux. Le soupçon de contrefaçon est éveillé par un ratio anormal entre l'effectif de la population de l'organisme et le nombre de licences acquises pour certains logiciels d'usage universel.

7. Préservation de l'intégrité des systèmes informatiques

Les virus et autres malfaisances informatiques par le réseau constituent une menace de sécurité omniprésente. Il n'y a pas de parade absolument sûre, mais la diminution du risque lié à cette menace passe par les recommandations suivantes :

- L'anti-virus du poste de travail doit être à jour et activé ;
- Le pare-feu du poste de travail doit être activé ;
- Les sites de divertissement sont un important vecteur de malfaisances de toutes sortes, leur visite doit être évitée depuis un poste de travail professionnel qui abrite des données sensibles ;
- Les logiciels de jeu et d'échanges de fichiers musicaux ou vidéo doivent, pour les mêmes raisons, être évités ;
- Les échanges de fichiers musicaux ou vidéo exposent en outre ceux qui s'y adonnent à des poursuites des ayant-droits des œuvres en question, dont les droits de propriété intellectuelle ne sont pas toujours respectés ;