Monsieur Thierry CHARPENTIER
SARL TH.CHARPENTIER
28,Rue plaine des Gardes
FR10300 - SAINTE-SAVINE
+33(0).25.74.50.73

à Madame / Monsieur DUPONT Jean

1,boulevard Charles Baltet

10000 TROYES

Sainte-Savine le 26112018 à 14:18:01,

OBJET : RAPPORT DE L'AUDIT RÉFÉRENCÉ SOUS LE N.° *49AEC5F6DC*

Après traitement des réponses que vous avez bien voulu apporter au questionnaire n°49aec5f6dc, nous avons plaisir à vous adresser le rapport d'audit afférent accompagné de nos recommandations d'actions.

Pour mémoire cet audit a pour valeur intrinsèque la qualité des réponses que vous avez pu y apporter, il est issu de la norme ISO 17799, elle même issue de la norme britannique BS 7799.

La norme 17799 fournit ainsi un canevas permettant d'identifier et de mettre en oeuvre des solutions pour les risques suivants :

- Politique de sécurité (Security Policy) : rédiger et faire connaître la politique de l'entreprise en matière de sécurité,
- Organisation de la sécurité (Security Organisation) : Définition des rôles et des responsabilités. Mise sous contrôle des partenaires et de l'activité externalisée,
- Classification des biens et contrôle (Asset Classification and Control) : Etat des lieux des biens de l'entreprise et définition de leur criticité et du risque associé,
- Sécurité du personnel (Personnel Security) : Embauche, formation et sensibilisation à la sécurité,
- Sécurité physique et environnementale (Physical and Environmental Security); Périmètre de sécurité, état des lieux des équipements de sécurité,
- Management des communications / Opérations (Comm / Ops Management) : Procédures en cas d'accident, plan de reprise, définition des niveaux de service et des temps de reprise, protection contre les malwares, etc.
- Contrôle d'accès (Access Control) : Mise en place de contrôles d'accès à différents niveaux (systèmes, réseaux, bâtiments, etc.),
- Développement et maintenance des systèmes (System Development and Maintenance) : prise en compte des notions de sécurité dans les systèmes de la conception à la maintenance,
- Planification de la continuité de l'entreprise (Business Continuity Planning) : Définitions des besoins en matière de disponibilité, des temps de reprise et mise en place d'exercices de secours,
- Conformité (Compliance) : Respect des droits d'auteur, de la législation et de la politique règlementaire de l'entreprise.

Nous restons bien entendu à votre entière disposition afin de collaborer avec-vous à la réussite de votre projet de sécurisation de votre infrastucture informatique

Veuillez touver ici Madame / Monsieur Jean DUPONT l'expression de nos courtoises salutations.

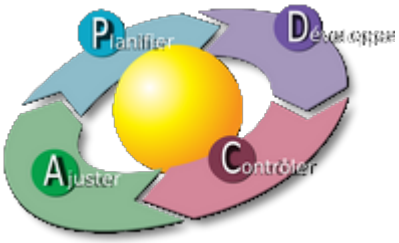
Vous en souhaitant bonne réception.

Thierry CHARPENTIER

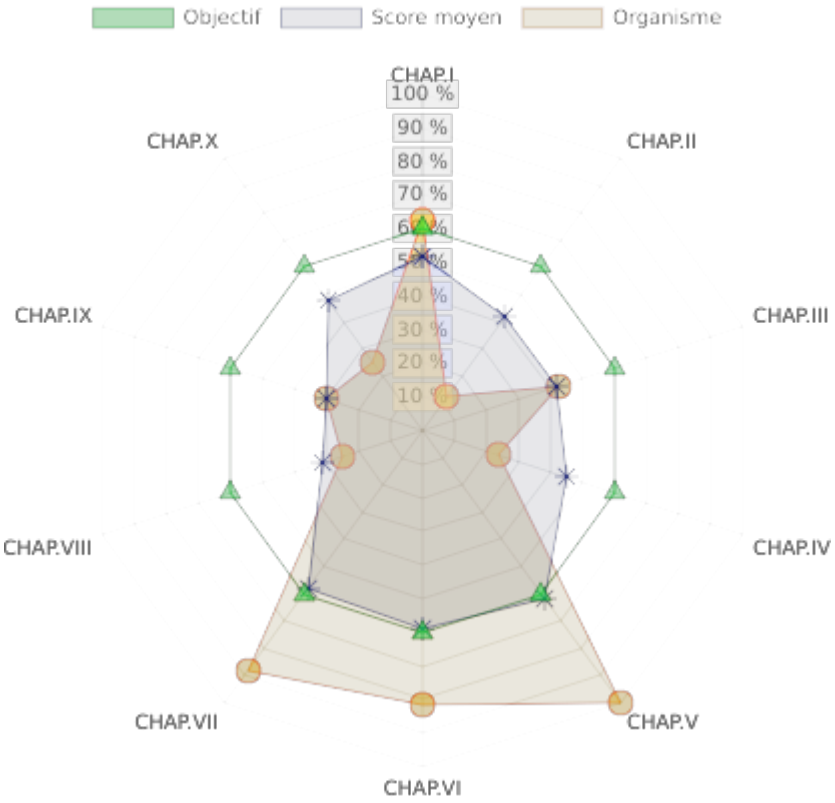
Th. Charpentier

COMPARATIF PAR SECTEURS D'ACTIVITES

Secteurs	Note globale
Administration	43,80%
Banque et assurance	57,20%
Commerce	47,40%
Communication	49,90%
Industrie	48,30%
Sante	44,40%
Services	55,20%
Moy. Générale	52,00%
Votre organisme	60,00%



RADAR



Référence de l'audit : 49aec5f6dc

RECOMMANDATIONS D'ACTIONS

I - POLITIQUE DE SÉCURITÉ INFORMATIQUE	L'implémentation de ce chapître de la sécurité est satisfaisante.
II - ORGANISATION DE LA SÉCURITÉ INFORMATIQUE	Ce chapître de la sécurité est à implémenter de manière urgente.
III - CLASSIFICATION ET CONTRÔLE DES ACTIFS	Ce chapître de la sécurité est à implémenter de façon prioritaire.
IV - SÉCURITÉ LIÉE AU PERSONNEL	Ce chapître de la sécurité est à implémenter de manière urgente.
V - SÉCURITÉ PHYSIQUE ET SÉCURITÉ DE L'ENVIRONNEMENT	L'implémentation de ce chapître de la sécurité est satisfaisante.
VI - SÉCURITÉ DE L'EXPLOITATION ET DES RÉSEAUX	L'implémentation de ce chapître de la sécurité est satisfaisante.
VII - CONTRÔLE D'ACCÈS LOGIQUES	L'implémentation de ce chapître de la sécurité est satisfaisante.
VIII - DÉVELOPPEMENT ET MAINTENANCE DE LOGICIELS	Ce chapître de la sécurité est à implémenter de manière urgente.
IX - CONTINUITÉ D'ACTIVITÉ	Ce chapître de la sécurité est à implémenter de façon prioritaire.
X - CONFORMITÉS	Ce chapître de la sécurité est à implémenter de manière urgente.

SYNTHÈSE DE L'ÉVALUATION

	Votre score	Score moyen	Objectif	
I - POLITIQUE DE SÉCURITÉ INFORMATIQUE	62,50%	52,00%	60,00%	*En France 2/3 des entreprises n'ont pas défini de politique de sécurité (source: CLUSIF 2003). Elles ne sont que 1/3 à ne pas l'avoir fait aux USA.*
II - ORGANISATION DE LA SÉCURITÉ INFORMATIQUE	12,50%	43,00%	60,00%	*44% des entreprises françaises ont, au moins, une personne chargée de la sécutié informatique. C'est souvent un spécialiste technique qui a une vision plutôt techno-centrique du sujet.*
III - CLASSIFICATION ET CONTRÔLE DES ACTIFS	42,53%	44,00%	60,00%	*La démarche d'identification des actifs d'information, des risques associés n'est encore diffusée que dans les grandes entreprises. C'est pourtant la base d'une démarche sécurité.*
IV - SÉCURITÉ LIÉE AU PERSONNEL	23,81%	44,00%	60,00%	*C'est un sujet peu abordé en France (alors qu'au moins 85% des attaques viennent de l'intérieur de l'entreprise), sauf sous le biais de sessions de sensibilisation, dont l'efficacité reste à démontrer*
V - SÉCURITÉ PHYSIQUE ET SÉCURITÉ DE L'ENVIRONNEMENT	100,00%	63,00%	60,00%	*C'est évidemment le sujet de la sécurité le mieux traité, car domaine plus technique qu'organisationnel et pris en compte depuis l'ouverture des premiers systèmes centraux.*
VI - SÉCURITÉ DE L'EXPLOITATION ET DES RÉSEAUX	81,25%	58,00%	60,00%	*Ce domaine est généralement au coeur des préoccupation de l'homme sécurité. Avec l'ouverture des réseaux aux clients et aux fournisseurs, la signature électronnique est promise à un bel avenir*
VII - CONTRÔLE D'ACCÈS LOGIQUES	88,37%	56,00%	60,00%	*Si évidemment il s'agit là d'une brique de base de la sécurité, organiser la revue des autorisations et complèter les mots de passe par un moyen d'authentification plus solide est très souvent utile.*
VIII - DÉVELOPPEMENT ET MAINTENANCE DE LOGICIELS	25,00%	43,00%	60,00%	*Domaine complexe, notamment lors de l'utilisation de progiciels (ERP, ...). A traiter lors de la mise en oeuvre d'@commerce ou en cas de dévellopement spécifiques sur le coeur de métier.*
IX - CONTINUITÉ D'ACTIVITÉ	30,00%	41,00%	60,00%	*plus de 70% des entreprises n'ont pas ou ne remettent pas à jour un plan de continuité d'activité.* *Pourtant il peut impliquer (ou non) la survie de l'entreprise en cas de sinistre majeur.*
X - CONFORMITÉS	25,00%	47,00%	60,00%	*Entre CNIL, DCSSSI, code pénal, ... les entreprises seraient avisées de mieux se protéger personnellement et de mettre en place une charte de sécurité (ou d'utilisation des TIC).*