AUDIT DE CYBERSÉCURITÉ – ÉTUDE DE CAS POUR LA PME

Auteur : Pascale Dominique, CISA, CRISC, CPA-CA, V-P Formation-Certification ISACA-Section Montréal.
(Note de l'auteur – Les guides de cybersécurité dont je fais référence dans cet article ne sont pas disponibles en français, les traductions sont des traductions libres)

Il faut être souple dans la définition d'audit de cybersécurité particulièrement dans le cadre d'un mandat en PME! Notre équipe multidisciplinaire évolue en sécurité et en technologie de l'information depuis plus de 25 ans, nous conseillons les clients pour qu'ils profitent des nouvelles technologies dans le maintien de leur positionnement stratégique. Notre mandat d'audit de la cybersécurité auprès d'une PME a comme objectif d'évaluer et de proposer des recommandations sur l'état du périmètre du réseau et de la cybersécurité; d'orienter et de conseiller notre client en matière de bonnes pratiques de l'industrie; et finalement de proposer un plan d'action pour corriger les faiblesses et vulnérabilités retracées et ainsi réduire les risques liés à la cybersécurité.
Étant membre de l'ISACA (Information Systems Audit and Control Association) - Section de Montréal, je cherche à apporter un levier et une plus-value en présentant au client un rapport cohérant et où des recommandations très techniques sont appuyées par des normes de bonnes pratiques et d'où découle le plan d'action. Cela facilitera la compréhension pour les chefs d'entreprise car pour la PME cela n'est pas toujours une mince affaire!
Dans ce contexte, nous aurons recours à des guides de bonnes pratiques pour la PME développés par l'ISACA et aux programmes de cybersécurité du National Institue of Standard and Technology (NIST) [1], qui favorisent le développement et l'application de technologies et de méthodologies de sécurité pratiques et innovantes pour l'amélioration des infrastructures critiques de cybersécurité.

EN PREMIÈRE PARTIE – UTILISATION DES GUIDES DE CYBERSÉCURITÉ

Les guides de cybersécurité pour la PME [2] proposés par l'ISACA sont des ressources incontournables. Ces guides s'alignent au référentiel COBIT 5 tout en adressant les besoins de la PME dont les ressources techniques et les budgets sont souvent limités. Le guide « Cybersecurity Guidance for Small and Medium-sized Enterprises » définit d'abord les différentes catégories de PME puis propose 8 principes et 55 clauses d'orientation (exigences/contrôles). Chacune des clauses reçoit une cote d'audit « Élevé » « Sévère » et « Important » identifiant un niveau de risque de cybersécurité pour une PME, voir **Table 1**.

[1] NIST, *Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity V1.1*, USA 2017
[2] ISACA, *Cybersecurity Guidance for Small and Medium-sized Enterprises*, USA, 2015
ISACA, *Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises*, USA 2015
ISACA, *Transforming Cybersecurity*, USA, 2013

Explication des notes d'audit	
Cote	**Explication**
Élevé	Impact majeur ou risque pour l'entreprise, mettant potentiellement en péril l'existence de l'entreprise. Les impacts et les risques peuvent être financiers, opérationnels, de réputation ou de toute autre nature.
Sévère	Impact significatif ou risque pour l'entreprise, avec d'importantes conséquences potentielles au cours de l'exercice
Important	Impact ou risque pour l'entreprise qui va au-delà des niveaux tolérés d'impact et de risque, tels que définis par la direction générale

Table 1 - Explication des notes d'audit

Chaque exigence est ensuite associée à une des cotes. La **Table 2** présente un exemple de quelques-unes des exigences qui sont ressorties au cours d'un mandat.

Exigences de cybersécurité vérifiables		
Clause d'orientation sur la cybersécurité (COC)	**Exigences/Contrôles**	**Cote**
1	Règles de gouvernance de cybersécurité documentées	Élevé
4	Stratégie de cybersécurité documentée	Sévère
11	Procédures documentées et pratiques de gestion	Important
21	Inventaire des actifs informationnels documenté/ classification des actifs informationnels, du risque de cybersécurité et les menaces	Sévère

Table 2 - Exigences de cybersécurité vérifiables

Une fois nos tests et analyses complétés, nous élaborons des recommandations pour les lacunes, faiblesses, ou vulnérabilités retracées et les priorisons de 1 à 3. En établissant une correspondance entre chacune de nos recommandations à une ou plusieurs clauses du guide - voir quelques exemples à la **Table 3 - Correspondance des exigences et des recommandations,** nous ajoutons une cohérence au rapport.

C.O.C.	Exigences/Contrôles	Cote	Recommandations	Priorité
1	Règles de gouvernance de cyber sécurité documentées	Élevé	R1	2
34	Configuration sécurisée des points d'entrée logiques	Élevé	R5-R6-R9	1
37	Mécanismes de défense contre les logiciels malveillants	Élevé	R7	3
38	Mécanismes de défense du périmètre	Élevé	R3-R4-R5-R6-R9	1
44	Les principes du « besoin d'en connaître » et du « moindre privilège » sont documentés et en évidence	Élevé	R8	3
4	Stratégie de cybersécurité documentée	Sévère	R1	1
21	Inventaire des actifs informationnels documenté/ classification des actifs informationnels, du risque de cybersécurité et les menaces	Sévère	R2	1
23	Identifier les infrastructures critiques, les applicatifs et services critiques ainsi que les services offerts par des	Sévère	R2	2

C.O.C.	Exigences/Contrôles	Cote	Recommandations	Priorité
	tiers qui sont critiques			
24	L'architecture de cyber sécurité est adéquate en fonction de la taille et complexité de l'entreprise	Important	R3	2
25	Compétences et aptitudes adéquates du personnel de cybersécurité	Important	R2	1

Table 3 - Correspondance des exigences et des recommandations

Finalement, nous faisons un rapprochement entre les recommandations et priorités proposées aux clauses d'orientation des exigences et contrôles, qui sont les critères d'exigences minimales pour des PME. La **Table 4 - Sommaire des recommandations par priorité et cote**, est un exemple du résultat obtenu.

Priorité	Cote	No recommandations	Recommandations	Exigences/Contrôles	C.O.C.
1	Élevé	R5	Rehaussement et revue de la configuration des routeurs	Configuration sécurisée des points d'entrée logiques	34
		R6	Mur pare-feu		
		R9	Protection contre les logiciels malveillants		
		R3	Complexité du réseau actuel	Mécanismes de défense du périmètre	38
		R4	Le réseau sans fil		
		R5-R6-R9	Rehaussement et revue de la configuration des routeurs /Mur pare-feu /Protection contre les logiciels malveillants		
2	Élevé	R5-R6-R9		Mécanismes permettant de sécuriser les actifs informationnels (appareils/logiciels et applications)	31
2	Sévère	R4-R5-R6-R9		Mécanisme de configuration sécurisée pour les périphériques réseau en y incluant les sous-traitants	33
2	Sévère	R4-R5-R6-R7-R9		Identifier les vulnérabilités	35
1	Sévère	R1	Absence de documentation formelle quant aux principes et politiques de sécurité	Stratégie de cybersécurité documentée	4
2	Élevé			Règles de gouvernance de cyber sécurité documentées	1
2	Important			Procédures documentées et pratiques de gestion	11

Table 4 - Sommaire des recommandations par priorité et cote

La Table 4 nous sert de base de travail pour faciliter la discussion et la prise de décision quant au plan d'action pour l'implantation des recommandations proposées et des mesures correctives à apporter aux contrôles internes.

EN DEUXIÈME PARTIE – MISE EN PLACE DES RECOMMANDATIONS ET MAINTIEN DES INFRASTRUCTURES CRITIQUES DE CYBERSÉCURITÉ

Le plan d'action mis en place permettra de maintenir la disponibilité, l'intégrité et la confidentialité des systèmes, en considérant trois grands axes : 1- une bonne gouvernance en alignant les objectifs des TI aux objectifs d'entreprises, 2- une gestion des risques jugés acceptables face à l'atteinte des objectifs établis, et 3- l'utilisation adéquate des ressources de l'entreprise. Pour réaliser cela, notre méthodologie s'appuiera sur le modèle du NIST pour l'amélioration des infrastructures critiques de cybersécurité de l'entreprise. Ce modèle est adaptatif et s'intègre au référentiel et processus de COBIT 5 pour sa mise en œuvre. Basé sur les risques, il est utilisé avec un large éventail de processus qui intègrent les opérations journalières en les regroupant en 5 fonctions tel que présenté à la **Figure 1- Fonctions du NIST CSF "Framework Core"**.

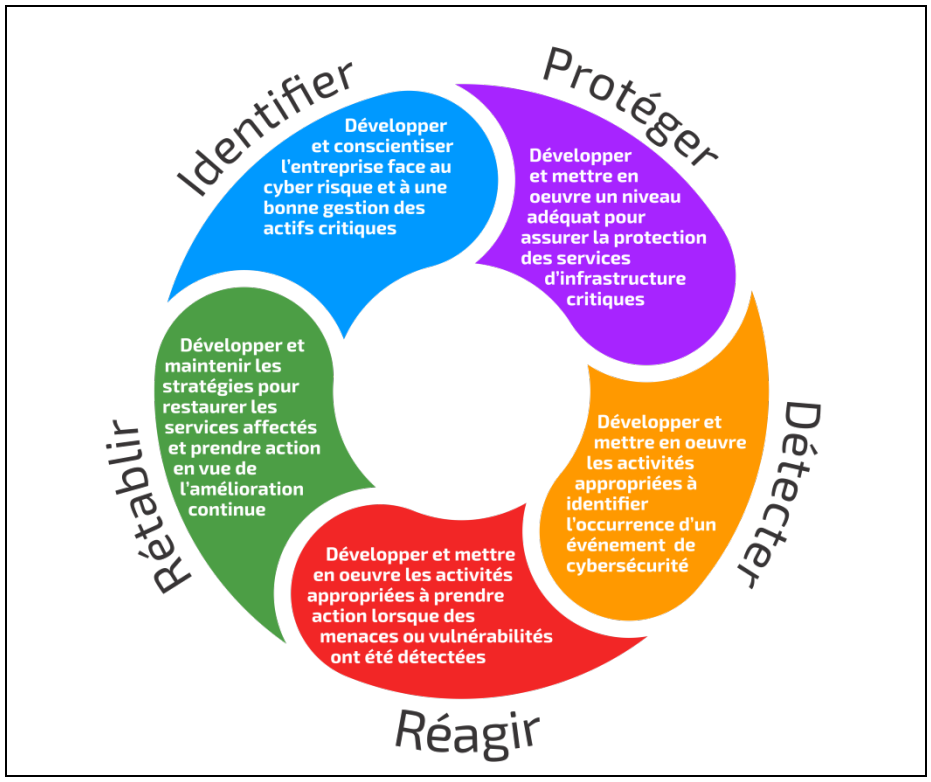

Figure 1- Fonctions du NIST CSF "Framework Core"

A haut niveau, ces fonctions permettent :

- L'identification des actifs critiques de l'entreprise;
- La protection des données qu'ils détiennent;
- La détection d'anomalies et d'incidents dans les systèmes;
- La réaction menant à des actions, des suivis et des améliorations continues aux systèmes et processus lorsque des menaces ou vulnérabilités ont été constatées;
- Le recouvrement lors d'incidents, les suivis et actions à prendre pour l'amélioration en rétroaction.

Dans cette perspective, la stratégie privilégiée pour sécuriser les systèmes d'information intégrera des mesures permettant de protéger les actifs critiques à un coût raisonnable pour l'entreprise.

Cette méthodologie qui intègre des pratiques largement utilisées dans l'industrie, est l'essence de notre pratique professionnelle car elle nous permet de bien servir nos clients et de rehausser la sécurité de leurs infrastructures critiques.

Pour plus d'information sur l'audit de cybersécurité, consultez notre site à https://www.connectalk.com/fr/infrastructure-et-securite/