12. Question de Emin ÖZKARA, conseiller communal, du 15 mars 2021 -=- Vraag van de heer Emin ÖZKARA, gemeenteraadslid, van 15 maart 2021.

Les services de cybersécurité pour les services publics communaux.

"Le Centre pour la Cybersécurité Belgique (CCB) offre une gamme de services de cybersécurité [CYBERSECURITY TESTS PEN] que les services publics fédéraux peuvent utiliser gratuitement. Chaque année, une évaluation est faite pour savoir quels services gouvernementaux peuvent utiliser ces tests de cybersécurité.

Les candidatures pour 2021 ont déjà été clôturées."

Je souhaiterais vous poser les questions suivantes :

1. À l'instar du CYBERSECURITY TESTS PEN proposé par la CCB aux services publics fédéraux, un test de cybersécurité est-il réalisé gratuitement et annuellement pour les services publics communaux ? Si oui, qui réalise ces tests ? De quand datent les derniers tests réalisés ? Des vulnérabilités ont-elles été découvertes ? Si oui, ces vulnérabilités ont-elles été traitées depuis lors?
2. Des services publics communaux ont-ils fait appel à l'expertise du CCB pour réaliser un CYBERSECURITY TESTS PEN ? Si oui, quels sont les services concernés?
3. En matière de sécurité informatique, de quand datent les dernières évaluations et audits au niveau de l'Informatique communale. Les politiques de sécurité des services publics communaux sont-elles à jour?
4. Enfin, quels sont les budgets réservés à la sécurité informatique de l'Informatique communale. Ce budget est-il suffisant eu égard aux enjeux colossaux en rapport avec l'intégrité, la confidentialité et la disponibilité des données numériques dans nos sociétés du tout numérique?

Réponse :

1) Concernant la question 1 – Test Cybersecurity Tests Pen :

Le Test PEN dont il est question dans votre demande ne s'applique pas aux Administrations Communales.

Il est conçu et réalisé gratuitement uniquement pour des organisations fédérales, dont la liste est disponible sur le site du SPF BOSA[1].

2) Concernant la question 2 – Consultation du CCB :

Les services communaux n'ont pas eu recours au service du CCB.

3) Concernant la question 3 – Les politiques de sécurité :

Notre équipe IT dispose en interne des profils nécessaires à la gestion et à la sécurisation des systèmes informatiques.

Plus particulièrement, nous avons deux agents au sein de l'IT qui occupent respectivement les postes suivantes :

- Un ingénieur « Réseaux » avec une formation relative aux règles de sécurités et à la sécurisation des infrastructures et réussie auprès de centre « Cisco[2] » ;
- Un ingénieur « Systèmes » & « Security Architect » qui, par ses formations et son expérience, assure un audit permanent de la sécurité de nos systèmes ainsi qu'une évaluation des risques pour chaque nouveau produit/projet au sein de notre infrastructure.

[1] https://fedweb.belgium.be/fr/a_propos_de_l_organisation/administration_federale/apercu_des_organisations_federales
[2] https://www.cisco.com/c/fr_be/training-events.html

- Notre infrastructure elle-même est conçue pour limiter les risques.

[Informations masquées pour des raisons de sécurité - NDA]

[redacted][3]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]

  [redacted][4].
- [redacted][5].

  [redacted]
- [redacted]

- Il va de soi que tous les systèmes listés ci-dessus sont continuellement mis à jour et renforcés dès qu'une amélioration est disponibles.

  La liste des budgets alloués à la sécurité (voyez question n°4) montre que les investissements dans ce domaine sont continus et gérés avec beaucoup de sérieux.
- Toutefois, il faut garder à l'esprit que la cyber sécurité ne concerne pas uniquement les systèmes, réseaux et autres logiciels. En effet, dans la pratique, le risque le plus important n'est pas externe mais bien interne, en raison du facteur humain.

  La grande majorité des attaques ou des intrusions est due à des actions effectuées par des utilisateurs internes soit par ignorance des risques, soit en toute connaissance de cause (acte illicite et soumis à des sanctions disciplinaire)[6].

---

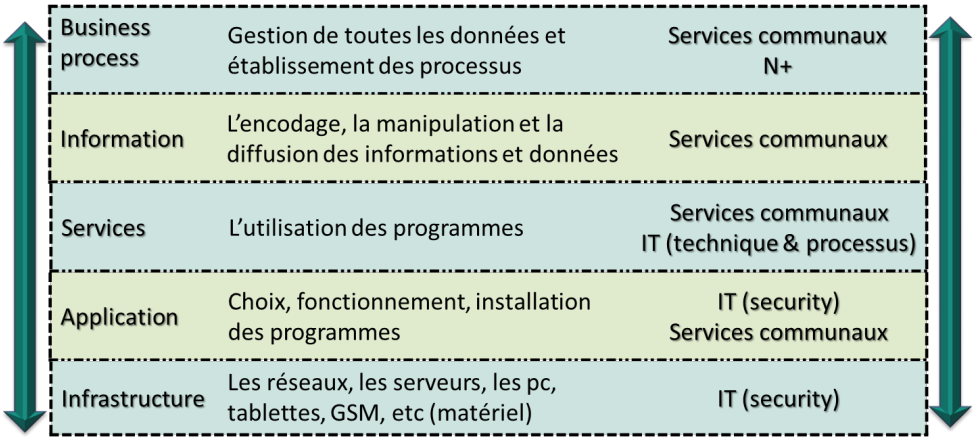
[3] [redacted]

[4] Pour plus d'informations : https://safeonweb.be/index.php/fr/actualite/les-mots-de-passe-cest-depasse

[5] La cote de 10/10 n'existe par principe pas vu qu'il est hypothétique voire utopique d'avoir des sentiments sécurisés à 100% car le risque existe et existera toujours même s'il est limité.

[6] Heureusement quasi inexistant actuellement vu qu'aucun cas n'a été signalé

Le rôle de chacun dans la lutte contre le cyber risque peut se modéliser ainsi :



Ce qui est souvent représenté par l'allégorie de « la Maison Cyber-sécurité », ainsi :

- L'IT est l'entrepreneur qui construit les fondations, les murs, les fenêtres, les portes, …
- Les agents sont les habitants de celle-ci et qui donc l'utilisent ;
  - ➔ Avoir une porte blindée ne sert à rien si on ne la ferme pas et inversement, quelle est l'utilité de fermer une porte qui est en contreplaquée ;
  - ➔ La cyber-sécurité est donc bien le travail de tous mais l'IT a en réalité un rôle plus limité qu'on ne le pense.

En conséquence, la priorité absolue doit rester la formation des utilisateurs aux bonnes pratiques IT et leur conscientisation face aux risques qui circulent. Ce principe de communication et d'information est totalement fonctionnel au sein de l'AC-Schaerbeek.

Ainsi tant l'IT que le CISO-DPO communal s'efforce de remplir ce rôle :

- L'IT signale régulièrement aux agents les courriels « spam » reçus par plusieurs agents et qu'il ne faut donc surtout pas ouvrir ;
- L'IT rappelle à tout moment les bonnes pratiques ;
- Le CISO-DPO rappelle les bonnes pratiques lors de sa mission de conseils et d'avis auprès des services ;
- Le CISO-DPO donne une formation interne relatif au RGPD intitulée « Cyber-sécurité-Base de données-Vie privée ». Celle-ci est actuellement en suspens en raison du Covid vu qu'elle est difficile à donner en webinaire. Actuellement, il y a environ 300 agents déjà formés[7] et il y aura jusqu'à plus de 500 agents au total qui seront formés.

4) Concernant la question 4 – Budget

Concernant le budget attribué à la cyber sécurité, le service IT fourni le tableau suivant :

PRODUITS	HTVA	TTC	REMARQUES
Firewall UTM - Maintenance + Licences (annuel)	48.000,00 €	58.080,00 €	
Datacenter CIRB - Services + Hébergement (annuel)	70.000,00 €	84.700,00 €	
VPN - Licences [redacted] (budget annuel)	20.000,00 €	24.200,00 €	
Outils sécurité informatique	40.000,00 €	48.400,00 €	
[redacted] Security - Licences & Support (annuel)	71.672,00 €	86.723,12 €	licences achetées pour 2 ans, soit 143.344,- € HTVA
	249.672,00 €	**302.103,12 €**	

[7] Essentiellement des directions Finances, Affaires générales, RH, Population et Enseignement

Enfin, dans le cadre du budget relatif à la sécurité informatique, il faut aussi inclure l'assurance cyber protection de notre assureur, la société ETHIAS8.

Cette assurance ne couvre pas uniquement le risque de perte physique du matériel et la responsabilité civile de la Commune, elle couvre aussi le risque quant à la perte des données et toutes conséquences dues aux cyber- attaques.

Ainsi, le sous-traitant d'ETHIAS fourni dans ce dernier cas une aide pour obvier ces derniers risques ; ce qui a allège la charge de travail pour le service IT lors de ces urgences et la Commune est accompagné d'experts externes.

Cette assurance inclut aussi une protection juridique.

Le budget attribué à cette assurance est de 16.800€.

[8] https://www.ethias.be/pro/fr/public/assurances/cyberprotection.html