MUNICIPALITÉ DE
NYON

PRÉAVIS N° 2022/32
AU CONSEIL COMMUNAL

Cybersécurité : renforcement de la sécurité des systèmes informatiques et d'informations

Demande d'un crédit d'investissement de CHF 908'000.- TTC

Demande d'un crédit supplémentaire au budget de fonctionnement de CHF 687'000.- TTC

Demande d'un crédit supplémentaire de CHF 130'000.- pour la création d'un nouveau poste d'informaticien à 100%

Délégué municipal : M. le Syndic Daniel Rossellat

Ire séance de la commission

Date	Jeudi 3 mars 2022, 19h30
Lieu	Salle de la Bretèche

Madame la Présidente,
Mesdames et Messieurs les Conseillers,

1. Introduction

Aujourd'hui, la sécurité de nos données est un enjeu majeur pour l'ensemble de la société. Elle implique une cohérence de l'ensemble du système d'informations avec comme objectif commun que chacun ait accès efficacement aux informations dont il a besoin.

Pour rappel, la sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'informations.

Ces dernières années, le nombre de cyberattaques n'a cessé d'augmenter. Celles-ci sont de plus en plus sophistiquées et touchent de plus en plus les entreprises, bien entendu, mais également les collectivités publiques. L'année dernière, plusieurs affaires de piratage ont été largement médiatisées (notamment celles des communes de Rolle et de Montreux) et ont créé un émoi légitime dans de nombreuses communes et autres administrations vaudoises, voire très certainement bien au-delà.

Heureusement, la Municipalité de Nyon, à travers son Office des solutions informatiques (OSI), n'a pas attendu ces récentes attaques pour sécuriser au maximum le réseau et les infrastructures informatiques de l'administration.

1.1 Anticipation et renforcement de la sécurité

Début 2021, la Municipalité a décidé de lancer une analyse préliminaire afin de déterminer l'état de la sécurité du système informatique et des systèmes d'informations de la Ville.

Cette première analyse a mis en lumière un état général des installations informatiques communales globalement bon, mais pouvant somme toute être amélioré.

C'est pourquoi la Municipalité a pris des mesures immédiates visant à renforcer la sécurité du système, notamment en sollicitant la réalisation d'un audit plus détaillé et approfondi des systèmes d'information et des installations dans leur ensemble auprès d'une entreprise spécialisée en gouvernance et sécurité informatique.

1.2 Etat des lieux et recommandations

Pour des raisons évidentes de sécurité, il n'est pas possible de détailler l'ensemble des résultats de cet audit. C'est pourquoi, sans rentrer dans les détails, il convient de souligner que les installations informatiques de la ville présentent certaines failles et vulnérabilités (situées à différents niveaux) et qu'en cas d'attaque, ces failles pourraient engendrer des risques relativement importants pour la Ville et les données de ses administrés.

Les mandataires ont pu, sur la base de leur analyse, formuler une série de recommandations quant aux mesures et solutions à déployer pour assurer à la Ville une sécurité globale du système. De leurs recommandations découlent précisément plusieurs mesures concrètes et prioritaires qu'il est impératif de déployer. Elles font l'objet de la présente demande de crédits soumise au Conseil communal et sont détaillées dans les pages suivantes.

2. Description du projet

2.1 Mesures de renforcement de la sécurité

A noter au préalable que les huit mesures présentées ci-après sont jugées comme complémentaires et indispensables, au risque sinon de ne sécuriser qu'une seule partie des infrastructures informatiques et de ne pas pouvoir assurer leur protection efficacement.

Mesure 1 : assurer la protection des e-mails entrants et Hardening DMARC

Pour rappel, près de 90 % des cybermenaces proviennent des systèmes de messagerie électronique. Le nombre de cyberattaques augmente continuellement et celles-ci sont de plus en plus sophistiquées. Les attaques les plus courantes sont le SPAM et le PHISHING. Dans la grande majorité des cas, c'est par la messagerie que les hackers exploitent leurs victimes en se présentant à elles sous une fausse identité pour les mettre en confiance et les encourager à répondre à leur message.

Les actions concrètes à déployer afin d'assurer la protection des e-mails sont :

1. installer un système de sécurisation des 800 boîtes de messageries électroniques de la Ville qui permettrait de : bloquer les e-mails et fichiers qui contiennent des fichiers actifs, surveiller les pièces jointes et assurer une veille en continu afin de ne recevoir que ce qui est pertinent, tout en désactivant les menaces potentielles.

   A noter que, depuis le mois de juin dernier, l'Office des solutions informatiques (OSI) – via un mandataire spécialisé – a installé à l'essai un système de protection sur les boîtes e-mails afin d'identifier et éviter les attaques extérieures.

   Après plusieurs mois d'essai gratuit, il s'avère qu'il est particulièrement efficace et redoutable de disposer de ce type de logiciel. C'est pourquoi il est devenu indispensable, au vu des récents événements survenus dans d'autres communes, que la Ville se dote d'un tel logiciel d'une part ainsi que des compétences pour relever et analyser les alertes qu'il pourra remonter d'autre part ;

2. empêcher l'usurpation des personnes de la commune, avec des alertes dans les e-mails provenant d'adresses externes pour limiter l'erreur humaine (par ex. l'ouverture d'un fichier contaminé par un collaborateur) ;
3. bloquer les contenus dangereux et les liens légitimes pouvant devenir malveillants ;
4. notifier les utilisateurs lorsque les liens sont réécrits (faux liens qui redirigent sur un autre site que celui affiché) ;
5. être en capacité de voir les e-mails bloqués afin que les faux positifs soient libérés ;
6. protéger des impersonnifications (de l'utilisation par des tiers de @nyon.ch).

Mesure 2 : migrer sur Office 365, avec protection / configuration (hardening)

Office 365 Exchange Online est l'équivalent *Cloud* de la solution actuellement utilisée par la Ville.

Cette solution présente de nombreux avantages en termes de sécurité : pas de redondance ; invulnérable face aux *ransomwares* (logiciels informatiques malveillants, prenant en otage les données) ; aucun entretien matériel, ni de logiciel, ce qui réduit drastiquement les attaques possibles ; déploiement des mises à jour et installation des dernières versions automatiquement par Microsoft ; en cas d'attaque, le hacker ne pourra pas effacer complétement ses traces, etc. Finalement, il n'y a pas de durée de vie limite nécessitant de renouveler l'infrastructure. Au

contraire, avoir un serveur physique coûte cher. Il s'agit de matériel coûteux qu'il faut renouveler tous les cinq ans et qui doit être en permanence maintenu afin d'offrir la disponibilité et la sécurité exigée.

Pour s'assurer d'une sécurisation complète des accès via *Office 365*, il est recommandé de protéger les utilisateurs aussi lorsqu'ils explorent Internet d'une part, et de configurer correctement la sécurité d'Office 365 tout en monitorant les événements d'autre part. En sus, il deviendra impératif que les utilisateurs s'authentifient en deux étapes (double authentification).

Mesure 3 : protéger les endpoints (points d'entrée) des réseaux informatiques que sont les appareils électroniques (PC, laptops, smartphones, tablettes, etc.).

Pour faire face aux menaces, la Ville doit opter pour des technologies de défense 24/7 afin de garantir :

- le blocage des tentatives de désinstallations des solutions de protection installées sur les ordinateurs des collaborateurs ;
- l'exploitation de toutes les fonctionnalités et les moyens de protections proposées par les solutions (chaque fonctionnalité non activée est une porte d'entrée pour les hackers) ;
- l'interprétation des alertes et des erreurs pour assurer le bon fonctionnement des protections ;
- une réaction proactive lorsqu'un incident se produira avec un *Endpoint Detection and Response* (l'installation d'une technologie *antimalware* afin de détecter les menaces et supprimer les logiciels malveillants).

Mesure 4 : mettre en place une gestion des informations et des événements de sécurité (SIEM)

Afin de pouvoir comprendre les incidents et les actions effectuées, et de pouvoir intervenir en bénéficiant d'une compréhension élargie, la mise en place d'un SIEM est déterminante. En effet, toute action sur un ordinateur crée une trace. En analysant ces informations, il est possible de détecter les événements inhabituels, suspects et dangereux très rapidement et efficacement. Un SIEM permettrait ainsi de remonter les actions suspectes d'un appareil électronique qui agit sur le réseau en corrélant les différentes informations provenant des points d'entrées avec les différents outils et systèmes de sécurité afin de pouvoir comprendre l'attaque et ses actions de façon efficace.

Mesure 5 : former et sensibiliser les utilisateurs

L'humain est un acteur essentiel de la sécurité, par sa capacité à mettre en œuvre les bonnes pratiques et à adopter une bonne cyber-hygiène. L'objectif est ici que les différents collaborateurs et acteurs de la Ville de Nyon puisse devenir les maillons forts de la protection face aux cyberattaques (tests en situation réelle, formation sur les fichiers reçus, sur l'usage des clés USB ou sur les nouvelles menaces, campagne de phishing, etc.).

Mesure 6 : sécuriser les connexions à distance sur les laptops de la Ville

La pandémie COVID-19 a bouleversé les fonctionnements et il a fallu réagir proactivement pour permettre le télétravail et ainsi réduire les contacts physiques. Pour ce faire, l'OSI a déployé des tunnels sécurisés (VPN) pour que les collaborateurs puissent se connecter depuis chez eux à l'infrastructure via des laptops fournis par la Ville.

Les hackers ont compris qu'ils peuvent utiliser ces équipements pour voler les identifiants de connexions à distance et ainsi accéder aux infrastructures.

Le Mobile Device Management (MDM) permettra de forcer des configurations,de gérer à distance les appareils et de pousser les politiques de sécurité, afin d'assurer que, même en transit, les règles de sécurité s'appliquent. La Data Loss Prevention (DLP) est quant à elle une solution qui protégera la Ville contre de potentielles exfiltrations de données et permettra de monitorer les données et ainsi de savoir à quel endroit se situe une donnée.

Mesure 7 : établir un Plan de continuité et un Plan de reprise

Ce n'est pas parce que tous les bons outils ont été mis en place pour se protéger qu'il ne convient pas d'anticiper un incident. Le concept du backup semble simple, mais comporte de nombreux challenges afin d'être mis correctement en place et de s'assurer que les données nécessaires seront disponibles en cas de besoin. Afin de mettre en place un Plan de continuité et un Plan de reprise, il est judicieux de pouvoir convertir un backup en système vivant et dans les meilleurs délais. Cette procédure permet ainsi d'assurer un plan de continuité afin que les services puissent continuer à fonctionner malgré le dérangement sur les serveurs.

Mesure 8 : Renouvellement des Switchs et routeurs de la Ville

Il est recommandé de renouveler les Switchs LAN de la Ville afin d'avoir un parc homogène de dernière génération plus facile à gérer et de mettre en place un contrat de maintenance avec un fournisseur pour garder un parc « up to date » et une réactivité en cas de problème.

2.2 Renforcement de l'Office des solutions informatiques (OSI)

Finalement, dans le but de mener à bien ce projet et la mise en œuvre des mesures de protection précitées, un renforcement des effectifs internes de l'Office des solutions informatiques (OSI) est à prévoir sous la forme :

- d'une consolidation de l'effectif de l'OSI pour assurer la gestion, le monitoring, le suivi, le contrôle et la maintenance des nouvelles applications (1 EPT) ;
- d'un mandat de prestations et d'accompagnement (soutien à l'élaboration et au lancement des appels d'offre, aide ponctuelle, suivi du projet, etc.).

L'objectif est d'assurer la meilleure mise en œuvre du projet et de soutenir l'équipe informatique et le responsable sécurité pour permettre le meilleur déploiement des différentes mesures dans le cadre du renforcement de la sécurité des systèmes informatiques et d'informations de la Ville.

3. Incidences financières

Les coûts de réalisation de ce projet ont été estimés sur la base d'applications existantes sur le marché pouvant répondre aux besoins et d'offres de fournisseurs et prestataires potentiels.

A noter en précision que toutes les exigences en termes de marchés publics seront respectées.

Coûts d'investissements

Frais de configuration / installation protection e-mails	CHF 2'900.-
Frais de configuration / installation Hardening DMARC	CHF 1'900.-
Migration et accompagnement Office 365	CHF 85'000.-
Frais de configuration / installation Office 365	CHF 8'800.-
Frais de configuration / installation *Endpoint Detection and Response*	CHF 4'900.-
Frais de configuration / installation SIEM	CHF 9'900.-

Formation et sensibilisation	CHF 60'000.-
Création plan de continuité et plan de reprise	CHF 12'000.-
Renouvellement et mise en place des Switchs	CHF 440'000.-
Mandat de prestations et d'accompagnement	CHF 200'000.-
Divers et imprévus (10%)	CHF 82'600.-
Total	**CHF 908'000.-**

Coûts de fonctionnement

Dès 2022, sous réserve de l'acceptation par le Conseil communal, ce projet impactera les budgets de fonctionnement 2022 et suivants de l'Office des solutions informatiques de la manière suivante :

Mesure	**Licences**	**Prestations de service**	**Total**
Protection e-mails	CHF 15'600.-	CHF 32'400.-	CHF 48'000
Hardening DMARC	CHF 5'500.-	CHF 11'500.-	CHF 17'000.-
Licences Office 365	CHF 201'000.-	-	CHF 201'000.-
Protection Office 365 (proxy web et hardening/monitoring)	CHF 65'000.-	CHF 67'000.-	CHF 132'000.-
Protection *Endpoint Detection and Response*	CHF 55'000.-	CHF 25'000.-	CHF 80'000.-
SIEM	CHF 60'000.-	CHF 70'000.-	CHF 130'000.-
Sécurisation à distance des laptops (MDM)	CHF 14'000.-	-	CHF 14'000.-
Plan de continuité et plan de reprise	CHF.60'000.-	CHF 5'000.-	CHF 65'000.-
Total	**CHF 476'100.-**	**CHF 210'900.-**	**CHF 687'000.-**

Renfort Office informatique (1 EPT)	**CHF 130'000.-**

4. Conclusion

Aujourd'hui, la sécurité des données et des installations informatiques est un enjeu majeur pour l'ensemble de la société. Ces dernières années, le nombre de cyberattaques n'a cessé d'augmenter, et plusieurs piratages ont récemment été largement médiatisés (dont notamment celles des communes de Rolle et de Montreux).

Quand bien même la Municipalité de Nyon n'a pas attendu ces récentes attaques pour sécuriser un maximum le réseau et les infrastructures informatiques de l'administration, il s'avère que l'état actuel de l'infrastructure informatique de la Ville est considérée à risque et qu'il est impératif que les mesures détaillées dans la présente demande de crédits soient déployées pour limiter au maximum le nombre de vulnérabilités possibles.

Au vu de ce qui précède, la Municipalité vous demande, Madame la Présidente, Mesdames et Messieurs les Conseillers, de prendre les décisions suivantes :

Le Conseil communal de Nyon

vu le préavis N° 2022/32 concernant « Cybersécurité : renforcement de la sécurité des systèmes informatiques et d'informations »,

ouï le rapport de la commission chargée de l'étude de cet objet,

attendu que ledit objet a été régulièrement porté à l'ordre du jour,

décide :

1. de valider la mise en place des mesures suivantes de renforcement de la protection des installations et systèmes informatiques de l'administration communale :
   - assurer la protection des emails entrants et Hardening DMARC ;
   - migrer sur *Office 365*, avec protection / configuration (hardening) ;
   - protéger les *endpoints* (points d'entrée) des réseaux informatiques que sont les appareils électroniques (PC, laptops, smartphones, tablettes, etc.) ;
   - mettre en place d'une gestion des informations et des événements de sécurité (SIEM) ;
   - former et sensibiliser les utilisateurs ;
   - sécuriser les connexions à distance sur les laptops de la Ville ;
   - établir un Plan de continuité et un Plan de reprise ;
   - renouveler les Switchs et routeurs de la Ville ;

2. d'accorder à la Municipalité un crédit d'investissement de CHF 908'000.- TTC destiné à la réalisation, la configuration et l'installation des mesures de renforcement de la sécurité informatique ;

3. de porter ce montant en augmentation du compte N° 9143.20 – *Dépenses du patrimoine administratif*, dépense amortissable en 10 ans ;

4. d'accorder à la Municipalité un crédit de fonctionnement supplémentaire de CHF 687'000.- TTC au budget 2022 pour financer les frais de fonctionnement des mesures de renforcement de la sécurité informatique, en augmentation du compte N° 190.3157.00 – *Entretien matériel et logiciel informatique* pour un montant de CHF 476'100.- et du compte N° 190.3185.01 – *Honoraires, frais d'assistance* pour un montant de CHF 210'900.- ;

5. d'accorder à la Municipalité un crédit supplémentaire de CHF 130'000.- au budget 2022, en augmentation des comptes N° 190.3011.00 – *Traitements* et suivants, afin de financer la création d'un poste à 100% pour renforcer l'effectif de l'Office des solutions informatiques ;

6. de prendre acte que la Municipalité inscrira ces montants aux budgets 2023 et suivants.

Ainsi adopté par la Municipalité dans sa séance du 10 janvier 2022 pour être soumis à l'approbation du Conseil communal.

Au nom de la Municipalité

Le Syndic : La Secrétaire a.i. :

Daniel Rossellat Marianne Savary

Annexe

- Tableau d'investissement

FICHE D'INVESTISSEMENT

PREAVIS No. 2022/32 — **Cybersécurité: renforcement de la sécurité des systèmes informatiques et d'informations** — **Date: Nyon le 19.01.2022**

Demande d'un crédit d'investissement de CHF 908'000 TTC

Situation des préavis au 19.01.2022	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Total des préavis votés par le Conseil communal	26 344 802	13 472 665	5 252 306	30 968 925	35 018 470	0

Situation des emprunts au 19.01.2022	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Plafond d'emprunt selon préavis N°2021/15	360 000 000	360 000 000	360 000 000	360 000 000	360 000 000	380 000 000
Emprunts au 1er janvier	213 000 000	263 000 000	289 000 000	297 500 000	291 300 000	281 300 000
Evolution des emprunts durant la période +/-	50 000 000	26 000 000	8 500 000	-6 200 000	-10 000 000	0
Emprunts fin période/date du jour	263 000 000	289 000 000	297 500 000	291 300 000	281 300 000	281 300 000

Cautionnements et garanties	
Plafond (préavis N°2021/15)	30 000 000
Caution activée	-9 229 230
Caution demandée	0
Disponible	20 770 770

Dépenses et recettes d'investissement		**Estimation des dépenses d'investissements nets**					
	CHF	**2022**	**2023**	**2024**	**2025**	**2026**	**2022-2026**
Descriptif/Libellé							
Diverses mesures de sécurisation	908 000	908 000	0	0	0	0	908 000
Total de l'investissement	**908 000**	**908 000**	**0**	**0**	**0**	**0**	**908 000**

Estimation amort. + entretien		
Durée ans	**Montant Amortiss.**	**Entretien annuel**
10	**90 800**	
	908 000	

Financement du préavis	**CHF**
Budget de fonctionnement:	
Trésorerie courante	
Investissement:	
Emprunts	908 000
Total des besoins en financement	

Coûts d'exploitation		**Estimation des coûts d'exploitation**					
Libellé / années		**2022**	**2023**	**2024**	**2025**	**2026**	**2022-2026**
Coût total d'exploitation		**835 160**	**925 960**	**925 960**	**925 960**	**925 960**	**4 539 000**
Intérêts en %	2,00%	18 160	18 160	18 160	18 160	18 160	90 800
Entretien		687 000	687 000	687 000	687 000	687 000	3 435 000
Amortissements		0	90 800	90 800	90 800	90 800	363 200
Personnel supp. en CHF		130 000	130 000	130 000	130 000	130 000	650 000
Personnel supp. en EPT		1,00	1,00	1,00	1,00	1,00	1,00
Recettes		**0**	**0**	**0**	**0**	**0**	**0**
Recettes		0	0	0	0	0	0
Coûts nets d'exploitation		**835 160**	**925 960**	**925 960**	**925 960**	**925 960**	**4 539 000**