MUNICIPALITE

PREAVIS N° 03/2023
AU CONSEIL COMMUNAL

Demande de crédit de CHF 250'000.—
pour le renouvellement et renforcement des équipements assurant la sécurité informatique du réseau de la Ville

Commissions	Date - heure	Lieu
Ad hoc	Me 8 février 2023 à 18h30	Hôtel-de-Ville, salle 6
Finances - COFI	Me 25 janvier 2023 à 18h15	Selon convocation

Vevey, le 16 janvier 2023

Monsieur le Président, Mesdames, Messieurs,

Introduction

Le Service des systèmes d'information a fortement renforcé les mesures de sécurité informatique ces dernières années. Sans rentrer trop dans les détails, étant donné que ce document est public, les mesures de sécurité suivantes ont notamment été adoptées :

- campagne reconduite annuellement de formation des utilisateurs·rices de la Ville sur les menaces et la cybersécurité en général
- tests de pénétration effectués par une société de sécurité depuis l'extérieur et l'intérieur du réseau afin de trouver d'éventuelles faiblesses qui sont documentées pour permettre des corrections ensuite ; ces tests vont dorénavant être pratiqués sur une base annuelle
- accompagnement par un consultant en sécurité
- durcissement des règles concernant la sécurité des mots de passe (longueur, remplacement régulier) basées sur les normes ISO 27000
- mise en place de l'authentification 2 facteurs pour les accès externes (là où c'est possible)

Ces mesures s'ajoutent aux systèmes de protection déjà en place depuis des années que sont les antivirus sur les postes de travail, les pare-feux, le filtrage des URLs et le système antispam.

Le présent projet s'inscrit dans le cadre de ce renforcement des systèmes et mesures de sécurité. Il prévoit le remplacement des deux pare-feux qui travaillent en tandem pour contrôler les flux réseau entre internet et le réseau de la Ville. Ces équipements, constitués de serveurs physiques dédiés (= des appliances) et d'un logiciel spécialisé, auront 4 ans au printemps 2023 et le prix de leur maintenance a augmenté fortement la troisième année. De plus, le Service des systèmes d'information entend protéger davantage les serveurs et les données de la Ville en renforçant les contrôles effectués par les pare-feux, ce qui exigera davantage de puissance de la part de ceux-ci et va ainsi forcer à remplacer les machines actuelles.

Parallèlement la Ville utilise pour le filtrage des spams et des virus une solution qui a donné globalement satisfaction et dont le prix est très avantageux. Toutefois, ce système n'incorpore pas les dernières techniques de protection (sandboxing, "désarmement" des pièces jointes, etc.) qui constitueraient clairement un plus pour empêcher des messages contenant des liens trompeurs, des virus, des ransomware ou des tentatives d'arnaque de parvenir jusque dans les boîtes des utilisatrices et utilisateurs. Le Service des systèmes d'information souhaite donc installer une solution plus performante afin de mieux protéger la messagerie de la Ville qui constitue un des points d'entrée principaux potentiels pour les menaces informatiques.

Situation actuelle

La passerelle de messagerie de la Ville est constituée d'un simple logiciel tournant sur un serveur virtuel. Cette solution contrôle tous les messages en arrivée à l'aide d'un moteur d'antivirus classique basé sur des signatures. Elle filtre également les spams sur la base d'une note attribuée aux serveurs d'envoi et aux expéditeurs. Ce filtrage manque malheureusement de paramétrage et la seule intervention pour des spams qui ne sont pas retenus est, à part signaler à l'éditeur de l'application ces courriels, de blacklister l'adresse d'envoi. Ce système de blacklist est malheureusement rarement efficace comme les spammeurs ne cessent pas de changer d'adresses d'envoi.

Les deux pare-feux actuels ont été achetés au printemps 2019. Ils travaillent en mode actif/passif, l'un d'eux assurant le filtrage et le deuxième étant prêt à prendre le relai en cas de défaillance du premier. Ces systèmes sont constitués par un logiciel qui tourne sur un serveur dédié et spécialisé, appelé "appliance", lui aussi vendu par le constructeur/éditeur. Il n'est donc pas possible d'augmenter les capacités de traitement de ces machines sans les remplacer totalement par des nouveaux modèles.

Grandes lignes et description de la modernisation projetée

Comme déjà indiqué le système qui joue le rôle de passerelle de messagerie et filtre le courrier entrant, si elle est une solution avantageuse financièrement, ne fournit pas les dernières avancées de certains produits concurrents quant aux fonctionnalités et capacités de filtrage. En effet, des solutions comme par exemple Fortigate ou Barracuda, sont capables de "désarmer" les fichiers dangereux (notamment en désactivant les macros ou les fichiers exécutables) et de vérifier l'innocuité d'un fichier en le faisant tourner dans un environnement "bac à sable" séparé de l'exploitation. Ainsi, même si une partie importante de la sécurité repose sur l'utilisateur·rice derrière son clavier, raison pour laquelle nous travaillons avec des cours en ligne de sensibilisation et formation aux cybermenaces, il convient néanmoins de limiter autant que possible les risques en stoppant les menaces en amont. C'est ce rôle que doit jouer la passerelle de messagerie en arrêtant au maximum tant les virus, que les rançongiciels, spams ou tentatives d'hameçonnage, que ce soient des messages contenant des liens, des fichiers joints ou des simples textes trompeurs.

En ce qui concerne les pare-feux, l'idée est de renforcer leurs rôles et les contrôles qu'ils effectuent. Présentement les pare-feux protègent principalement le réseau interne de la Ville, dans lequel se trouvent les serveurs principaux, de l'extérieur soit des menaces venant d'internet. A l'avenir l'idée est de protéger les serveurs du réseau interne en faisant transiter également les accès internes par les pare-feux. Ceci exige par contre d'avoir des pare-feux plus puissants à même de traiter sans ralentissements le trafic interne qui est naturellement bien plus conséquent que le celui en provenance d'internet. Il faut aussi noter qu'une tentative d'accès sur les serveurs par un hacker qui serait parvenu à prendre à distance le contrôle d'un PC de la Ville ou à rentrer sur le réseau communal avec un accès VPN serait dès lors considéré comme un accès interne. Il est donc important de sécuriser également les accès internes.

Le Service des systèmes d'information veut ainsi acheter des pare-feux ayant des capacités de traitement plus importantes, afin de pouvoir mettre en place, sans provoquer de ralentissements, des règles de protection supplémentaires empêchant par exemple les accès aux serveurs en dehors des protocoles autorisés depuis le PC ou le VPN d'un utilisateur lambda qui aurait été hacké.

Objectifs de ce remplacement

Les objectifs de ce remplacement vont au-delà d'un remplacement un pour un des équipements et logiciels. La volonté du Service des Systèmes d'information est ainsi

d'augmenter la sécurité des systèmes informatiques de la Ville en mettant en place une nouvelle passerelle de messagerie permettant :

- d'améliorer le filtrage des cybermenaces en désarmant en temps réel les fichiers joints présentant des dangers ou les liens
- d'analyser dans un environnement de test (bac à sable), sans danger pour nos systèmes, les éventuelles menaces
- d'améliorer le filtrage des spams en fournissant également des possibilités de paramétrage plus étendu pour bloquer les pourriels échappant à l'antispam

Parallèlement le remplacement des pare-feux permettra :

- de renforcer la sécurité des serveurs en faisant transiter également par les pare-feux les accès à ceux-ci depuis l'intérieur du réseau informatique communal

Détail des coûts

Les coûts d'acquisition des équipements, des services d'installation et paramétrage, ainsi que de 5 ans de maintenance, sont les suivants :

Description	**Montant**
Achat des pare-feux (2 appliances redondantes, du logiciel et de 5 ans de maintenance)	CHF 150'000.--
Services d'installation et de configuration des pare-feux	CHF 10'000.--
Achat de la solution de passerelle de messagerie (hardware, licences, 5 ans de maintenance)	CHF 70'000.--
Services d'installation et de configuration de la passerelle de messagerie	CHF 10'000.--
Divers et imprévus	CHF 10'000.--
Total	CHF **250'000.--**

Il faut relever que si ces montants sont conséquents, les équipements et logiciels installés protégeront davantage les systèmes informatiques de la Ville et réduiront l'exposition de ceux-ci aux cybermenaces, même si évidemment la sécurité absolue n'existe pas dans ce domaine.

Quant à l'aspect prix, notons que les CHF 150'000.- couvrant l'achat des pare-feux, leur utilisation durant 5 ans et leur maintenance sur la même période représentent un montant annuel de CHF 30'000.- qu'il faut comparer avec les CHF 17'000.- de maintenance annuelle payés en 2022 pour les firewalls actuels. L'augmentation, ramenée à une charge annuelle, est donc limitée d'autant que celle-ci permet de financer également le remplacement du hardware.

En ce qui concerne la passerelle de messagerie, le coût de CHF 70'000.- pour l'utilisation et la maintenance de ces systèmes sur une période de 5 ans représente un coût annuel de CHF 14'000.-. Celui-ci est bien plus élevé que celui de la solution actuelle (un peu moins de CHF 2'500.-), mais comme indiqué précédemment le passage à une nouvelle génération de passerelle de messagerie renforcera considérablement la protection de celle-ci face aux virus, ransomwares, tentatives d'arnaques et spams. Le coût annuel semble aussi

raisonnable en regard de ceux des antivirus sur les postes et les serveurs (on parle plutôt d'EDR : Endpoint Detection and Response pour les solutions modernes comme celle installée à Vevey) et la campagne annuelle de sensibilisation du personnel qui sont tous deux du même ordre de grandeur.

A noter aussi que les montants demandés sont une enveloppe maximale basée sur des offres budgétaires. Le Service des systèmes d'information essaiera bien sûr d'obtenir les meilleurs prix en passant par deux appels d'offres pour les équipements différents que sont les pare-feux et la passerelle de messagerie, mettant ainsi en concurrence différents fournisseurs.

Aspect financier

Plan des investissements

Cet objet figure au plan des investissements 2022-2026 pour un montant total de CHF 300'000.--.

Ces coûts pour améliorer la protection des systèmes informatiques de la Ville sont toutefois raisonnables. Ils sont à mettre en rapport avec l'importance de l'informatique pour le fonctionnement des services communaux et de la Ville.

Financement

Le financement de cet investissement sera assuré par la trésorerie courante.

Charges financières

Dans le but de mieux évaluer la totalité des charges annuelles futures découlant d'un investissement, il y a lieu de tenir compte d'un montant comprenant à la fois l'amortissement et les intérêts.

Amortissement

Nous proposons d'amortir le crédit de CHF 250'000.-- demandé par le présent préavis par un amortissement linéaire d'environ 1/5 du montant total pendant 5 ans selon les normes du MCH2.

Conclusion

Le projet du Service des systèmes d'information est cohérent. Il prévoit d'avancer le remplacement des pare-feux de la Ville pour permettre l'acquisition et la mise en place de nouveaux équipements plus performants qui permettront de mieux protéger les serveurs et les données de la Ville. De plus, le coût de maintenance des firewalls actuels ayant fortement augmenté en quatrième année, l'objectif est de remplacer ceux-ci avant de devoir payer une 5ème année de maintenance. Pour éviter cette situation d'augmentation des maintenances au terme de la 3ème année, une maintenance de 5 ans sera directement achetée avec les nouveaux pare-feux.

En ce qui concerne la passerelle de messagerie, la solution en place depuis des années est vieillissante et n'intègre pas les dernières solutions de sécurité ("désarmement" des fichiers joints et liens potentiellement dangereux, sandboxing) pour protéger les boîtes de messagerie de la Ville. Même si les coûts de cette solution sont avantageux, il convient de renforcer les protections contre les cybermenaces en passant à un système plus moderne incorporant les techniques mentionnées précédemment.

La principale justification de ces deux opérations de renouvellement et renforcement des systèmes de sécurité que sont les pare-feux et la passerelle de messagerie filtrant les virus et les spam, réside bien sûr dans les menaces qui pèsent sur les systèmes informatiques des entreprises et de ceux des communes. Des attaques comme celles contre les communes de Rolle et de Montreux en 2021 sont malheureusement des illustrations de cette situation et les coûts de telles attaques peuvent être importants, notamment si elles entraînent plusieurs jours d'indisponibilité des systèmes informatiques, sans compter l'atteinte à l'image.

Le Service des systèmes d'information travaille donc à réduire autant que possible les risques pour les systèmes informatique par la formation du personnel communal, par des mesures de sécurité et par la modernisation des systèmes de protection, comme proposé dans ce préavis.

En conclusion, nous vous prions, Monsieur le Président, Mesdames, Messieurs, de bien vouloir prendre les décisions suivantes :

LE CONSEIL COMMUNAL DE VEVEY

VU le préavis N° 03/2023 du 16 janvier 2023, concernant la « Demande de crédit de CHF 250'000.— pour le renouvellement et renforcement des équipements assurant la sécurité informatique du réseau de la Ville » ;

VU le rapport de la commission chargée d'étudier cet objet, qui a été porté à l'ordre du jour ;

d é c i d e

1. d'allouer à la Municipalité un crédit de CHF 250'000.— pour financer le renouvellement des pare-feux et de la passerelle de messagerie ;

2. de financer cette dépense par la trésorerie courante, par prélèvement sur le compte "Dépenses d'investissements" ;

3. d'amortir cette dépense par un amortissement linéaire pendant 5 ans selon les normes du MCH2.

Au nom de la Municipalité

le Syndic	le Secrétaire
Yvan Luccarini	Grégoire Halter

Municipal délégué : M. Yvan Luccarini, Syndic

Annexe : Lexique

Petit lexique des termes informatiques (inspiré de Wikipédia):

Active Directory :
Système d'annuaire centralisant les données sur tous les "objets" (PC, imprimantes, comptes utilisateurs) du réseau. Il s'agit de l'architecture normale de gestion sous Windows 2000/2003 Serveur remplaçant les domaines de Windows NT.

Adresse IP (ou TCP/IP) :
Adresse unique sur Internet attribuée à chaque PC faisant partie d'un réseau.

Appliance :
Serveur prêt à l'emploi dédié à remplir une seule fonction. Sorte de boîte noire, il est plus simple à installer et à administrer, mais est bridé pour ne remplir que la tâche pour laquelle il a été conçu (par exemple Firewall ou serveur de Proxy).

Bit :
0 ou 1 en binaire. Elément d'information de base traité par l'ordinateur. 8 bits composent un octet (byte en anglais) et sont nécessaires pour coder un caractère alphanumérique. 1 Mbits = 1 million de bits. 1 Gbits = 1 milliard de bits.

Commutateur ou switch :
Equipement de communication "intelligent" utilisé pour interconnecter PC et serveurs via le câblage réseau. C'est une sorte de central téléphonique informatique.

Contrôleur de domaine :
Serveur gérant les comptes des utilisateurs et les droits d'accès sous les réseau Windows NT 4.0. Un serveur principal et un serveur secondaire conservent chacun une copie de la base des comptes utilisateurs et machines (structure remplacée par Active Directory).

DHCP (Dynamic Host Configuration Protocol) :
Système d'attribution automatique des adresses IP dans un réseau.

DNS (Domain Name Search) :
Recherche des noms de domaines Internet. On peut dire qu'il s'agit d'une sorte de système d'annuaire global (en fait de nombreux serveurs interconnectés) qui fournit l'adresse IP (adresse unique sur Internet) du site que l'internaute veut visiter.

Domaine :
Unité d'organisation par laquelle se gèrent les réseaux Microsoft. C'est au niveau du domaine que sont maintenus et contrôlés les comptes des utilisateurs et des machines.

EDR :
Endpoint Detection and Response. Antivirus de nouvelle génération sur les postes de travail et ne se basant plus uniquement sur des bases contenant des définitions de virus, mais capable d'analyser le comportement d'un programme et de bloquer son activité en cas d'opérations suspectes.

Firewall ou pare-feu :
Equipement de sécurité permettant de filtrer/contrôler les accès vers l'intérieur ou l'extérieur d'un réseau.

Flash :
La mémoire flash est une mémoire de masse à semi-conducteurs ré-inscriptible, c'est-à-dire une mémoire possédant les caractéristiques d'une mémoire vive mais dont les données ne

disparaissent pas lors d'une mise hors tension. Elle est utilisée tant pour les cartes mémoire USB, que pour les cartes d'appareil photo ou les disques SSD.

GBIC :
Module permettant d'interconnecter des équipements réseau via des fibres optiques à une vitesse très élevée (1 Gigabit/s).

GED (gestion électronique de documents)
Le terme GED désigne aussi bien un procédé informatisé visant à organiser et gérer des informations et des documents électroniques au sein d'une organisation que les logiciels utilisés pour le faire.

Gigabits/s ou Gbits/s
Débit de 1 milliard de bits par seconde, soit 125 Méga octets par seconde.

HTTP (Hyper Text Transfer Protocol) :
Protocole de gestion des transferts d'information de type web (navigation sur Internet).

Hyperconvergence (ou hyper-convergence) :
Architecture matérielle informatique qui lie les composants de traitement (processeurs et mémoire vive), de stockage (disques), de réseau et de virtualisation. L'hyperconvergence englobe les éléments d'infrastructure dans un pool de ressources partagées, en intégrant un stockage réparti sur différents nœuds.

Octet (=byte en anglais) :
1 octet = 8 bits. C'est l'unité de taille en informatique, un octet permettant de coder un caractère. 1 Mo = 1 Méga octets, soit 1 million d'octets. 1 Go = 1 Giga octets, soit 1 milliard d'octets. 1 Tera octets soit 1'000 milliards d'octets.

Hameçonnage (phishing en anglais) :
L'hameçonnage est une technique utilisée par des pirates pour obtenir des renseignements ou accès personnels, en faisant croire à la victime qu'elle s'adresse à un site ou une personne de confiance, dans le but de perpétrer une usurpation d'identité.

Pare-feu (firewall en anglais)
Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter selon des règles les communications autorisées sur un réseau informatique, notamment celles entrant et sortant de et vers internet. Il surveille et contrôle les applications et les flux de données (paquets).

Passerelle de messagerie (email gateway en anglais)
Une passerelle de messagerie est un logiciel et/ou un matériel qui fonctionne comme un pare-feu spécifique à la messagerie. Elle protège les serveurs de messagerie internes et les boîtes des utilisateurs·rices d'une organisation contre les contenus malveillants (virus, spams, rançongiciels, etc.) qui circulent à partir d'internet et tentent d'accéder aux systèmes.

Proxy :
Equipement fournissant un accès à Internet centralisé, permettant d'accélérer celui-ci par le biais de pages stockées en mémoire et d'enregistrer un journal unique des pages Internet consultées.

Rançongiciel (ransomware en anglais)
Un rançongiciel, aussi appelé logiciel de rançon ou logiciel d'extorsion, est un logiciel malveillant qui prend en otage des données personnelles ou d'entreprise. Pour ce faire, un rançongiciel va se lancer en toile de fond et chiffrer les données personnelles trouvées avant de demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Redondance
Dans le domaine informatique, la redondance n'est pas une tare mais une qualité qui permet d'assurer une excellente sécurité des systèmes, même si elle a un coût. La redondance des serveurs et des baies de stockage permet ainsi qu'un deuxième système prenne le relai (grâce aux mécanismes de la virtualisation géré par un serveur de pilotage) du premier en cas de défaillance de celui-ci.

Réplication
La réplication des données est la copie de celles-ci sur un autre équipement de stockage. Dans le projet présenté, la réplication des données principales se ferait entre des baies de stockage se trouvant sur deux sites, ce qui permettrait aussi bien de limiter les pertes de données en cas de problème sur un des sites, que de transférer rapidement l'activité sur le site non affecté.

RJ45 :
Prises réseau de type câblage universel.

Sandbox ou bac à sable
Un bac à sable (en l'anglais sandbox) est un mécanisme de sécurité informatique se basant sur l'isolation d'éléments suspects, comme certains types de fichiers en pièces jointes, pour les faire tourner et tester dans un environnement de test séparé sans danger pour les systèmes.

Snapshot
Un snapshot est une copie des données à un instant donné.

Spam ou pourriel :
Messages publicitaires électroniques non souhaités et le plus souvent au contenu problématique (par exemple vente de logiciels piratés, vente de médicaments en ligne, publicité pour des sites érotiques, etc.).

SMTP (Simple Mail Transfer Protocol) :
Protocole de transfert de courrier sur Internet.

SSD (solid-state drive) :
Matériel informatique permettant le stockage de données sur de la mémoire flash (=mémoires à semi-conducteurs à l'état solide) par opposition à la technologie plus ancienne des disques durs, sur lesquels les données sont écrites sur un support magnétique en rotation rapide.

TCP/IP :
Protocole réseau (=comme un langage avec ses règles et conventions de communication) utilisé d'abord sur Internet, qui s'est généralisé ensuite de façon quasi universelle dans les entreprises et chez les particuliers.

URL (Uniform Ressource Locator) :
Adresse globale d'une ressource sur internet (par exemple http://www.vevey.ch).

Virtualisation :
La virtualisation consiste à imiter complètement le fonctionnement d'un ou plusieurs serveurs physiques à l'aide d'un logiciel et d'en fournir toutes les fonctionnalités. Ceci permet de tirer parti de la puissance des serveurs actuels multicoeurs, capables de faire fonctionner une demi-douzaine de serveurs virtuels, et ceci en continuant de cloisonner les tâches en les répartissant entre les différents serveurs virtuels.

VLAN
Réseau virtuel qui permet de cloisonner des réseaux par le biais de filtres de sécurité mis en place sur des commutateurs. On peut ainsi par exemple définir un VLAN différent pour les serveurs et les PC, dans le but de protéger les systèmes centraux.

VMware :
Solution de virtualisation leader du marché.

VPN :
Pour Virtual Private Network, solution permettant l'accès au réseau interne de l'entreprise depuis une machine distante à travers un accès sécurisé transitant par internet.