Administration générale et culture

Renforcement de la sécurité des Systèmes d'Information pour la période 2016-2019

Préavis n° 2015/73

Lausanne, le 22 octobre 2015

Monsieur le président, Mesdames et Messieurs,

1. Objet du préavis

« Faire de l'infrastructure informatique une source de valeur ajoutée fiable pour la Ville de Lausanne »

Par le présent préavis, la Municipalité sollicite l'octroi d'un crédit d'investissement du patrimoine administratif de CHF 2'500'000.- afin, d'une part, de permettre le renforcement de la sécurité des Systèmes d'Information et, d'autre part, de diminuer les risques informatiques tout au long des années 2016 à 2019. Le présent préavis est dûment intégré au plan d'investissement 2016-2019, au nombre des crédits à voter de la direction Administration générale et culture, Service organisation et informatique, sous le titre préliminaire suivant : « Mise en place de mesures de diminution du risque et du pilotage de la sécurité des Systèmes d'Information ». Le début de l'investissement est prévu en 2016.

Les demandes présentées dans ce préavis visent à soutenir le développement de l'informatique de la Ville, tel que présenté dans le « schéma directeur des Systèmes d'Information 2013-2017 », et à diminuer les risques nouveaux. Ceux-ci sont induits par l'ouverture des Systèmes d'Information que la cyberadministration implique et par une mobilité des outils de travail de plus en plus marquée, voire exigée. Par ailleurs, les menaces organisées et ciblées étant courantes, il y a lieu d'être mieux préparé et de remettre constamment à jour les processus, les moyens… et nos certitudes.

2. Préambule

La digitalisation des Systèmes d'Information de la Ville de Lausanne n'a cessé d'évoluer depuis plus de quarante ans, au point de représenter aujourd'hui un outil indispensable à la conduite des missions de l'administration communale. C'est le cas dans toutes les administrations et entreprises modernes. Le taux de croissance annuel des éléments de l'infrastructure informatique montre à quel point celle-ci est chargée (serveurs : +15% par an, données : +40%, utilisation du réseau : +30%, etc.). Un préavis spécifique est présenté chaque législature afin d'encadrer cette croissance des infrastructures et de restreindre les choix technologiques.

Cette évolution ne concerne pas seulement l'informatique classique, mais aussi l'informatique technique. Les automates industriels sont également connectés sur le réseau informatique RECOLTE, surveillés et pilotés par des systèmes techniques de plus en plus proches de l'informatique classique. Ils représentent aujourd'hui plus de 60% des appareils connectés sur le réseau local. Cette automatisation s'étend à notre vie de tous les jours avec des équipements qui sont tous connectés : sondes, caméras, etc.

L'Internet, ainsi que l'ouverture des applications et des infrastructures vers le monde extérieur (citoyens, partenaires), alliés au confort apporté par la mobilité, participent à la modernisation et à « l'agilité » des nouveaux services offerts à la population. Cela facilite les tâches des différents collaborateurs et les rapports avec leurs partenaires.

Ce cadre évolutif augmente la sensibilité aux risques informatiques. Le Service d'organisation et d'informatique prend d'ores et déjà en charge ceux qui sont liés à l'organisation :

- un plan de développement des Systèmes d'Information, un comité de cadrage des évolutions informatiques, une conduite coordonnée des projets avec les autres services, ainsi qu'une volonté accrue de regroupement des solutions informatiques, amènent de la cohérence. Le but est d'appliquer et suivre une politique unique et normée avec une montée en maturité qui ne laisse aucun système de côté ;
- le récent renouvellement des salles informatiques a permis une importante diminution des risques précédemment encourus avec les anciennes salles et permet d'assurer une plus haute disponibilité des prestations informatiques de la Commune ;
- des équipements et systèmes de protection sont mis en œuvre dans le cadre des évolutions des Systèmes d'Information, de l'évolution du réseau RECOLTE ou des mesures prises après des audits de sécurité.

Cependant, ces actions ne suppriment pas tous les risques et plusieurs aspects ne sont pas encore suffisamment pris en compte :

- l'une des particularités de l'administration communale, vue comme une entreprise, est le nombre de locaux utilisés et leur diversité. Environ 500 sites sont informatisés, ou au moins disposent du réseau informatique RECOLTE. Il n'y a pas aujourd'hui un concept unique de sécurisation globale des locaux, ni même des armoires techniques qui abritent le câblage et donnent accès au réseau ;
- de nouvelles technologies apparaissent constamment, créant de nouveaux risques. Elles devraient être évaluées, homologuées, avant toute intégration dans l'environnement informatique de la Ville. Cette démarche systématique doit être imposée pour tous les équipements connectés, à un moment donné, au réseau informatique. La démarche concerne également les applications et services hébergés dans des environnements de type nuage (Cloud computing) ;
- les mondes personnel et professionnel s'entremêlent, à l'avantage de l'entreprise, mais aussi en ajoutant des risques importants. Les habitudes et expériences personnelles, acquises dans la vie privée, gagnent le monde du travail, créant un risque accru d'exposition, c'est-à-dire de divulgation, des données ;
- des menaces nouvelles, dont la nature varie constamment, apparaissent sans cesse. Les programmes informatiques malveillants (maliciels) sont devenus une arme facile à trouver ou acheter, aisément utilisée par les milieux criminels ou certains gouvernements. Ces menaces obligent à une vigilance constante.

Bien sûr, des méthodes et des normes de protection existent. Elles donnent un cadre de mise en œuvre des mesures de sécurité, ainsi que les « bonnes pratiques » de pilotage. La méthode choisie par la Ville est la suite de normes ISO27000. Cette politique générale a été entérinée en novembre 2007, sans qu'il s'en soit suivi un déploiement systématique, appuyé par des directives, des mesures de communication et de contrôle. De même en ce qui concerne les systèmes de protection et les bonnes pratiques de gestion de la disponibilité, qui n'ont pas été accompagnés par un suivi systématique des incidents de sécurité. C'est le volet ISO27001 de la norme qui cadre, en particulier, les systèmes de management de la sécurité de l'information (SMSI) et qu'il est nécessaire de mettre en place, avec la gouvernance associée.

3. Etat des lieux

3.1. Les protections mises en œuvre.

L'informatique de la Ville de Lausanne n'a cessé d'évoluer depuis plus de quarante ans, offrant plus de confort aux employés et un service plus rapide et plus fiable aux usagers.

Le Service d'organisation et d'informatique (SOI) a pris en compte et mis en place les outils et les bonnes pratiques en matière de protection. C'est une démarche incrémentale qui n'est pas forcément prévue dans tous les plans d'évolution. Si le SOI est attentif et inclut ces mesures dans les projets dont il a l'initiative, ce n'est pas le cas pour tous les projets de l'administration communale.

L'ensemble de ces mesures traite plusieurs enjeux de la sécurité de l'information, comme la confidentialité ou l'intégrité. S'agissant de la disponibilité en particulier, la construction de nouvelles salles informatiques et la redondance choisie pour les différentes infrastructures (réseau, calcul et stockage) permettent d'offrir un service stable. Les autres points ont des niveaux de maturité divers, relevés dans les audits conduits par le SOI, qu'il conviendrait d'adresser d'une manière plus globale comme la traçabilité, la conformité et la confidentialité.

3.2. Les attaques et la criminalité

La criminalité numérique s'est intensifiée avec l'Internet et de véritables stratégies alliant plusieurs techniques informatiques ou d'ingénierie sociale sont mises en œuvre pour soutirer de l'argent aux administrations, pour nuire à leur image, ou encore affecter leur capacité à délivrer leurs services. Il devient de plus en plus facile de pirater ou d'altérer des systèmes informatiques grâce aux programmes malveillants disponibles sur l'Internet. Les hackers ont les moyens, les compétences et le temps ; ils sont nombreux et ils sont de plus en plus audacieux. Chaque année, on recense davantage de cas. La plupart ne sont pas rendus publics.

Les attaques sont permanentes et, pour la plus grande partie, ne sont pas ciblées. Considérées comme un bruit ambiant, elles sont prises en charge par les éléments de protection en place. D'autres attaques, au contraire, ciblent régulièrement des organisations précises, plus ou moins grandes, et la Suisse ne fait pas figure d'exception.

Le tableau suivant liste quelques cas révélés, survenus en Suisse durant ces dernières années :

Date, media	***Attaques***	**Commentaires**
06.11.2009, RTS	Le Département fédéral des affaires étrangères (DFAE) piraté	Attaque d'une institution
Janvier 2014, Ouest-France, bilan.ch	BCGE : 30'000 e-mails de clients. Les hackers réclament €10'000.- pour ne pas les diffuser	Rançon
Février-mars 2014	Le virus Duqu a infecté les ordinateurs de la Confédération	Contexte international sur le nucléaire iranien
Juillet 2014, bcv.ch	Attaques de pirates informatiques contre les systèmes e-banking de banques suisses	Phishing/rançon
27.04.2015, lematin.ch	Les sites du Parti Chrétien-Social suisse et valaisan ont été hackés par un personnage ou un groupe se réclamant de l'EI	Atteinte à l'image en raison d'une opinion
07.05.2015, tdg.ch	Le site d'Implenia victime des hackers d'« Anonymous »	Accusation de prise de position pour la scientologie
13.05.2015, RTS	Virus informatique « Dyre »	Cible : comptes bancaires Plus de 2000 infections

10.06.2015, lemonde.fr	Espionnage des négociations sur le nucléaire iranien	Programme sophistiqué, pour la prise de contrôle d'équipements techniques
08.07.2015, letemps.ch	Attaques informatiques en série contre des avocats genevois. Plainte antérieure similaire	Affaire en justice liée à la Finance

La Ville de Lausanne n'échappe pas à ce phénomène et a fait l'objet d'attaques ou de menaces plus ou moins ciblées :

Date	***Evénement***
31.07.2012	Injection de code SQL malicieux dans l'application MUSERIS
03.09.2014	Tentative d'extorsion à la direction des SiL (ingénierie sociale)
09.12.2014	Infection d'un poste avec un « cryptolocker » qui a nécessité la restauration d'un volume de travail de groupe
17.04.2015	Trois postes infectés avec un virus mineur : exploitation du carnet d'adresses
14.07.2015	Menace via les réseaux sociaux et la presse d'un groupe se réclamant d'« Anonymous »
10.08.2015	Tentative d'extorsion à la direction des SiL (ingénierie sociale)

3.3. L'informatique technique

L'existence d'une informatique technique, toujours plus intégrée avec l'informatique de gestion, induit un risque important de deux points de vue. D'une part, c'est une cible de choix car, contrairement à l'informatique classique, la prise en compte de la sécurité est assez tardive, aggravée par un cycle de renouvellement des équipements plus long. D'autre part, les vulnérabilités et les absences de protection de nombre de ces équipements pourraient servir de cible et de tremplin aux programmes malveillants. Des aménagements architecturaux sont nécessaires, ainsi qu'un accompagnement plus rapproché des projets des différents services techniques de l'administration, afin de diminuer le risque jusqu'à un niveau acceptable.

Comme dans d'autres entreprises, des équipes différentes gèrent les réseaux de contrôle des processus, alors que le service informatique gère les autres réseaux. Cela engendre nécessairement des divergences dues à des priorités différentes et des procédés divergents, notamment sur le thème de la gestion des risques informatiques.

4. Les améliorations envisagées

4.1. Introduction

Les améliorations envisagées consistent à reprendre globalement la politique de sécurité, à harmoniser son niveau de maturité dans l'ensemble des domaines et à rendre l'ensemble cohérent en y intégrant une dimension relative à l'informatique technique et industrielle.

L'expérience de ces dernières années a montré non seulement qu'il n'était pas possible de procéder par incréments avec des actions d'urgence ensuite des différents audits, mais aussi que les moyens affectés à la sécurité des Systèmes d'Information n'étaient pas suffisants pour une administration comme celle de la Ville de Lausanne, qui cumule des compétences diversifiées, chacune avec ses contraintes, ses spécificités et ses modes de fonctionnement en matière de traitement de l'information.

4.2. Renforcement du fonctionnement des systèmes et des applications

Un ensemble de mesures organisationnelles et techniques visant à réduire les risques dans les différents domaines qui exposent le système d'information, doivent être mises en place :

- continuité, gestion de la disponibilité : ce sont des notions comprises dans la construction des data center, mais qui nécessitent organisation et vérification régulière ;
- classification des données et qualification des niveaux d'habilitation pour les accès ;
- extension et renforcement du contrôle d'accès des prestations en ligne, en réponse aux besoins d'ouverture des Systèmes d'Information ;
- ségrégation des réseaux, environnements et données, avec différenciation des usages et des règles d'accès ;
- mise en œuvre d'un plan spécifique de sécurisation des réseaux techniques ;
- sensibilisation des utilisateurs et tout particulièrement des professionnels de l'informatique ;
- conduite d'analyse de risques systématiques et application des mesures de mitigation ;
- modernisation des infrastructures et équipements assurant la sécurité, plusieurs aspects techniques n'étant pas mis en œuvre faute de moyens : détection d'intrusions, analyse comportementale ;
- modernisation des couches de sécurité applicative ;
- notion de contrôle d'accès au réseau (NAC) : risque élevé en raison du nombre de sites et de l'absence de contrôle d'accès systématique.

4.3 Contrôles et gestion des accès

Les accès aux éléments des systèmes d'information sont multiples et de formes diverses. Il y a aussi bien des accès physiques que des accès logiques, qui doivent tous deux être gérés de manière appropriée. Les processus de gestion ne sont qu'embryonnaires, prenant tout juste en compte les arrivées et départs des collaborateurs. Il conviendra de mener des analyses de risques dans ces différents domaines afin d'identifier précisément toutes les mesures à mettre en place.

Les analyses préliminaires effectuées nous permettent d'ores et déjà de formuler les améliorations impératives suivantes :

- contrôle d'accès physique ;
- contrôle d'accès au réseau ;
- gestion des droits d'accès (y compris cycle de vie) ;
- contrôle des droits d'administration ;
- mise en place d'une matrice de compatibilité des droits ;
- mise en œuvre de la gestion et du contrôle d'accès dans les environnements techniques.

4.4 Gouvernance

La gouvernance est une activité globale, qui prend en compte l'ensemble des projets, les tâches récurrentes, ainsi que la gestion des différents processus concernés. Les points suivants sont traités dans le cadre du présent préavis :

- organisation, définition des responsabilités et des procédures de la sécurité des Systèmes d'information ;
- conseil et accompagnement des projets des services de l'administration par le SOI ;
- formalisation d'un plan de gestion de crise et rapprochement avec le plan DIAM[1] ;
- centralisation et corrélation des événements ;
- système de management de la sécurité de l'information : ISO27001 (SMSI) ;

[1] Acronyme pour Directives d'Intervention en cas d'Accident Majeur de la Ville de Lausanne (DIAM). Ces directives prévoient un plan général de préparation des fonctions administratives concernées ainsi qu'un état-major inter-services, c'est le *Plan DIAM*.

- mise en œuvre de la prévention et de la détection d'intrusions ;
- gouvernance des données (classification des données, définition des responsables des données, référentiels de données, etc.)
- sensibilisation et formation des acteurs en fonction de leur(s) rôle(s) ;
- audit, prévention et analyses de risques : cartographie des risques ;
- conformité légale et au regard des règlements municipaux ;
- communication aux employés, aux externes concernés, aux autorités.

5. Détail des projets

Renforcement de la sécurité des systèmes et des applications	
Continuité	Analyse de risques Création et mise en œuvre d'un plan de continuité informatique Test et mise à jour des plans de continuité
Sécurité des données	Plan de classification Mesures de lutte contre la fuite de données Sécurité des systèmes de fichiers
Sécurité du développement	Sécurité des environnements de développement et de soutien aux applications (maintenance) Exigences de sécurité des systèmes Bonnes pratiques Standards Processus d'audit de code
Ségrégation	Ségrégation des réseaux Contrôle des connexions au réseau Contrôle du routage des réseaux Sécurité des services de réseau Cryptage des transmissions passant par le réseau Ségrégation des données
Rénovation des composants de sécurité	Socle IAM [2] Détection d'intrusions
Sécurisation des communications	Accords sur les échanges d'informations et de logiciels Sécurité des supports en transit Sécurité de la cyberadministration et du paiement électronique Sécurité du courrier électronique Sécurité des systèmes bureautiques Systèmes accessibles au public Autres formes d'échange d'informations
Mesures cryptographiques	Politique d'utilisation des mesures cryptographiques Cryptage Signatures numériques Services de non-répudiation ou non-dénégation Gestion des clés

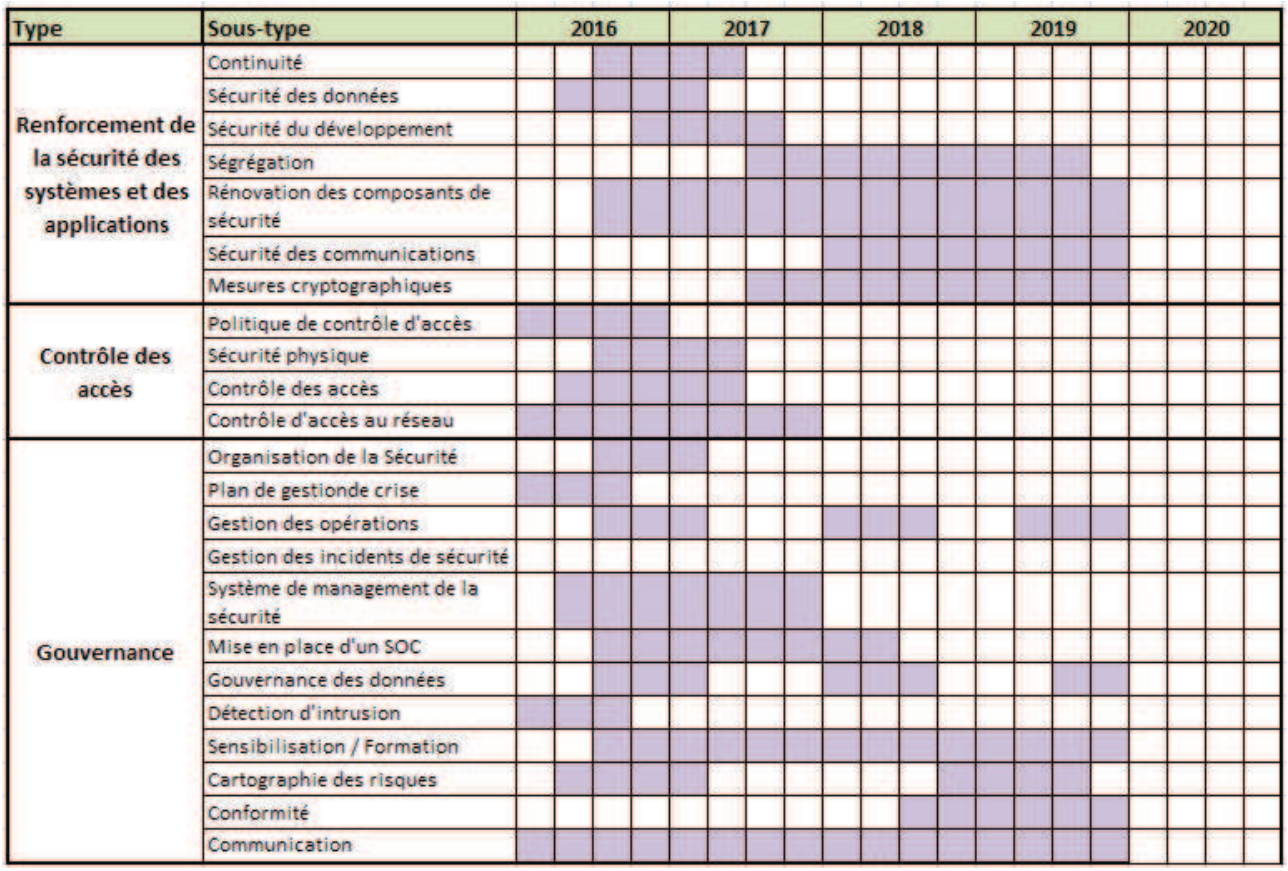
[2] IAM est l'acronyme de *Identity and Access Management*, à savoir l'ensemble des technologies d'identification et d'attribution de droits d'accès en matière informatique.

Contrôle des accès	
Politique de contrôle d'accès	Exigence de l'administration Responsabilité de l'utilisateur
Sécurité physique et de l'environnement	Zone de sécurité informatique Sécurité du matériel Mesures de contrôle général
Contrôle des accès	Gestion des accès utilisateurs Contrôle d'accès aux systèmes d'exploitation Contrôle d'accès aux applications Informatique mobile et télétravail Consignation des événements Séparation des responsabilités
Contrôle d'accès au réseau	Analyse de risques Sélection et mise en œuvre d'un outil (NAC) Politique d'utilisation des services de réseau Itinéraire obligatoire Authentification des nœuds Détection d'intrusions

Gouvernance	
Organisation de la sécurité	Audit de l'organisation en place Mise en place des rôles et responsabilités (y compris dans les services)
Conseil et accompagnement des projets Ville	
Plan de gestion de crise	Formalisation d'un plan de gestion de crise
Gestion des opérations	Procédures et responsabilités opérationnelles Planification et réception (recette) des systèmes Protection contre les logiciels pernicieux Intendance d'exploitation Gestion des réseaux Manutention et sécurisation des supports de données Echanges d'informations et de logiciels
Gestion des incidents de sécurité	Centralisation et corrélation des événements Traitement des événements Reporting
Système de management de la sécurité de l'information : ISO27001 (SMSI)	Mise en place d'un SMSI
Mise en place d'un SOC : Security Operation Center	

Mise en œuvre de la prévention et détection d'intrusions	Système, alerting [3], procédures
Gouvernance des données (classification, responsable des données, référentiels)	
Sensibilisation/Formation des acteurs Analyses de risques : Cartographie des risques	
Audit et prévention	
Conformité	Conformité aux exigences légales Politique de sécurité et conformité technique
Communication	

6. Planning prévisionnel



[3] En informatique, « alerting » se dit de l'ensemble des méthodes, procédures, définitions de l'urgence et de la criticité ainsi que du choix des destinataires d'alertes (ce terme allant du simple avertissement dont le traitement n'est pas obligatoire, jusqu'au blocage immédiat d'un système d'information).

7. Aspects financiers

7.1. Dépenses relatives à la sécurité de l'information

Avec l'évolution des infrastructures et des applications, la Ville s'est dotée, progressivement et dans le cadre de projets particuliers, du personnel de sécurité ainsi que d'équipements et solutions de sécurité. Cette approche incrémentale suivait les conclusions des audits successifs. La sécurité de l'information n'a pas fait l'objet, à ce jour, d'un plan global, articulé sur le moyen terme, sur une législature, ni non plus d'une dotation de moyens qui pourraient offrir sérénité et continuité dans la manière d'aborder les projets relatifs aux technologies de l'information. C'est d'autant plus vrai pour ce qui concerne la protection des données.

7.2. Investissements prévus pour la période 2016-2019

(en milliers de CHF)		Extensions			Frais récurrents
Type	***Sous-type***	***Matériel***	***Logiciels***	***Prestations***	
Renforcement de la sécurité des systèmes et des applications	Continuité			150	
	Sécurité des données	20	50		10
	Sécurité du développement	10	40	45	5
	Ségrégation	40	92	30	20
	Rénovation des composants de sécurité	50	185	30	30
	Sécurité des communications		30	20	
	Mesures cryptographiques		10	20	
	Sous-total	*120*	*407*	*295*	*65*
Contrôle des accès	Politique de contrôle d'accès			30	
	Sécurité physique	50	30	20	16
	Contrôle des accès		30	75	6
	Contrôle d'accès au réseau	50	250	50	50
	Sous-total	*100*	*310*	*175*	*72*
Gouvernance	Organisation de la sécurité			20	
	Plan de gestion de crise		10	30	
	Gestion des opérations		25	95	
	Gestion des incidents de sécurité	10	190	20	50
	Système de management de la sécurité		20	30	10
	Mise en place d'un SOC		20	30	
	Gouvernance des données	10	30	20	6
	Détection d'intrusions	15	65	20	10
	Sensibilisation / formation			80	
	Cartographie des risques			30	
	Conformité			90	
	Communication			20	
	Sous-total	*35*	*360*	*485*	*76*
TOTAUX		**255**	**1'077**	**955**	**213**

L'estimation de l'échelonnement des dépenses et des recettes est la suivante :

(en milliers de CHF)	2016	2017	2018	2019	2020	Total
Dépenses d'investissements	1'000	600	600	300	0	2'500
Recettes d'investissements	0	0	0	0	0	0
Total net	**1'000**	**600**	**600**	**300**	**0**	**2'500**

Les montants ci-dessus s'entendent toutes taxes comprises.

7.3. Incidences sur le budget de fonctionnement

7.3.1. Charges de fonctionnement

L'augmentation de l'activité, du volume de l'infrastructure et des nouveaux logiciels génèrera chaque année un surcroît de charges de fonctionnement qui sera absorbé dans l'enveloppe budgétaire ordinaire accordée au SOI.

7.3.2. Charges d'amortissement

Les charges d'amortissement prévues sur une durée de cinq ans, découlant de l'échelonnement des dépenses indiqué au paragraphe 7.2, s'élèvent à CHF 500'000.- par année à compter de 2017.

7.3.3. Charges d'intérêts

Calculés sur la base d'un taux d'intérêt moyen de 2.75%, les intérêts théoriques moyens développés par le présent préavis s'élèvent à CHF 37'900.- à compter de l'année 2017.

7.3.4. Tableau récapitulatif

Le tableau ci-après synthétise les éléments présentés aux paragraphes 7.3.1, 7.3.2 et 7.3.3 ci-dessus :

(en milliers de CHF)	2016	2017	2018	2019	2020	2021	Total
Personnel suppl. (en ept)	0	0	0	0	0	0	0
Charges de personnel	0	0	0	0	0	0	0
Autres charges de fonctionnement	0	0	0	0	0	0	0
Charges d'intérêts	0	37.9	37.9	37.9	37.9	37.9	189.5
Charges d'amortissement	0	500.0	500.0	500.0	500.0	500.0	2'500.0
Total charges suppl.	**0**	**537.9**	**537.9**	**537.9**	**537.9**	**537.9**	**2'689.5**
Diminution de charges	0	0	0	0	0	0	0
Revenus	0	0	0	0	0	0	0
Total net	**0**	**537.9**	**537.9**	**537.9**	**537.9**	**537.9**	**2'689.5**

8. Conclusions

Vu ce qui précède, nous vous proposons, Monsieur le président, Mesdames et Messieurs, de bien vouloir prendre les résolutions suivantes :

Le Conseil communal de Lausanne,

vu le préavis N° 2015/73 de la Municipalité du 22 octobre 2015;

ouï le rapport de la Commission nommée pour examiner cette affaire;

considérant que cet objet a été porté à l'ordre du jour,

décide :

1. d'allouer à la Municipalité un crédit d'investissement du patrimoine administratif de CHF 2'500’000.- destiné à couvrir les frais de renforcement de la sécurité des Systèmes d’Information pour la période 2016-2019 ;
2. d'amortir annuellement sur une durée de cinq ans le crédit prévu ci-dessus par la rubrique 1500.331 du budget de fonctionnement du Service d'organisation et d'informatique ;
3. de faire figurer au budget de fonctionnement du Service d'organisation et d'informatique les intérêts relatifs aux dépenses découlant du crédit figurant sous chiffre 1 ci-dessus sous la rubrique 1500.390.

Au nom de la Municipalité

Le syndic :
Daniel Brélaz

Le secrétaire :
Simon Affolter