

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

SESSION EXTRAORDINAIRE 2019

13 juin 2019

**Les élections simultanées du 26 mai 2019
pour le Parlement européen, la Chambre des
représentants et les Parlements de région et
communauté**

RAPPORT

DU COLLÈGE D'EXPERTS CHARGÉS DU CONTRÔLE
DU SYSTÈME DE VOTE ET DE DÉPOUILLEMENT
AUTOMATISÉS

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

BUITENGEWONE ZITTING 2019

13 juni 2019

**Gelijktijdige verkiezingen van 26 mei 2019
voor het Europees Parlement, de Kamer
van Volksvertegenwoordigers en de
Gemeenschaps- en Gewestparlementen**

VERSLAG

VAN HET COLLEGE VAN DESKUNDIGEN BELAST
MET DE CONTROLE VAN HET ELEKTRONISCH
STEM- EN STEMOPNEMINGSSYSTEEM

**Rapport du Collège d'experts chargés du contrôle des
systèmes électroniques de vote, de dépouillement et
de collecte des résultats**

**Élections simultanées du 26 mai 2019
pour le Parlement européen, la Chambre des
représentants et les Parlements de région et
communauté**

Bruxelles, le 7 juin 2019

Rapport du Collège d'experts – élections de 2019

Table des Matières

1	Le Collège	4
1.1	Composition du Collège	4
1.2	Le Collège non permanent.....	4
1.3	La mission.....	5
1.4	Le rapport.....	6
1.5	Secret	6
1.6	Mise à disposition des moyens nécessaires.....	6
2	Législation	7
2.1	Modifications concernant les systèmes de vote	7
2.2	Modifications concernant la publication des codes sources	7
2.3	Modifications concernant le Collège d'experts	7
3	Description des systèmes.....	8
3.1	Description fonctionnelle globale	8
3.2	SmartMatic.....	8
3.2.1	Description fonctionnelle.....	8
3.2.2	La procédure électorale avec preuve papier	9
3.2.3	Éléments techniques du système SmartMatic utilisé dans les bureaux de vote	10
3.3	Martine	11
3.3.1	Infrastructure	11
3.3.2	Logiciels.....	12
4	Contrôles et constatations	14
4.1	Contrôles effectués avant le jour des élections	14
4.1.1	Contrôles du système SmartMatic	14
4.1.2	Contrôle du système Martine – module MA2X.....	18
4.1.3	Relations entre les firmes responsables des développements	19
4.1.4	Analyse des codes sources	19
4.1.5	Analyse du CCB	20
4.1.6	Visite du Datacenter au SPF Intérieur	21
4.1.7	Participation aux séances de formation	21
4.1.8	Respect des procédures	22
4.2	Constatations le jour des élections	23
4.2.1	Contrôles dans les bureaux de vote	23
4.2.2	Incidents dans les bureaux de vote.....	25
4.2.3	Contrôles dans les bureaux principaux	26
4.2.4	Incident : Publication prématurée des résultats sur les sites Web des médias.	27
4.2.5	Incident de la transmission des résultats à partir des cantons le soir des élections	28
4.3	Contrôles effectués après le jour des élections.....	29
4.3.1	Vérification des totalisations	29
4.4	Diffusion du code source	32
4.4.1	Code source des logiciels SmartMatic.....	32
4.4.2	Code source du système Martine	32
5	Recommandations.....	33
5.1	Recommandations faisant suite au problème de transmission des résultats	33

Rapport du Collège d'experts – élections de 2019

5.2	Recommandations concernant les procédures	33
5.3	Recommandations faisant suite aux rapports du CCB	34
5.4	Recommandations générales	35
6	Conclusion	36

1 Le Collège

1.1 Composition du Collège

En application de l'article 24 de la loi du 7 février 2014 modifiée par la loi du 19 avril 2018 organisant le vote électronique avec preuve papier, les experts dont les noms suivent sont désignés pour une durée de 5 ans afin de composer le Collège permanent.

Experts désignés par la Chambre des représentants :

- effectifs : M. Bruno DE NYS, M. Karel VAN GEYT et M. Jérôme DOSSOGNE ;
- suppléants : Mme Sophie JONCKHEERE, M. Jean-Marc PAUL et M. Erwin VERECKEN.

Experts désignés par le Parlement flamand :

- effectif : M. Bart MARTENS ;
- suppléant : M. Romain VOES.

Experts désignés par le Parlement de la Région de Bruxelles-Capitale :

- effectif : M. Emmanuel WILLEMS ;
- suppléant : M. Pascal VAN de WALLE.

Experts désignés par le Parlement de la Communauté germanophone :

- effectif : M. Daniel BRANDT ;
- suppléante : Mme Susi SARLETTE OSTLENDER.

Ces experts constituent le Collège d'experts permanent.

Le Parlement wallon n'a désigné aucun expert pour ce Collège permanent.

Conformément à l'article 24 § 2 de la loi du 7 février 2014, les experts effectifs ont désigné en leur sein un président, M. Emmanuel WILLEMS, et un secrétaire, M. Bart MARTENS.

1.2 Le Collège non permanent

Conformément à l'article de l'article 24 § 3 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier, les experts dont les noms suivent sont désignés afin de composer le Collège non permanent à l'occasion des élections simultanées du 26 mai 2019 pour le Parlement européen, la Chambre des représentants et les Parlements de région et de communauté :

Experts désignés par la Chambre des représentants : M. Bruno PENNE et M. Pol BADOUX.

Experts désignés par le Parlement wallon : M. Jean-François DAMSEAUX et M. Alexandre BUBOIS.

Experts désignés par le Parlement flamand : M. Romeo MARYNS et M. Steven ES.

Rapport du Collège d'experts – élections de 2019

Experts désignés par le Parlement de la Région de Bruxelles-Capitale : M. Fabrice DUMORTIER et M. Jean-Michel DRICOT.

Experts désignés par le Parlement de la Communauté germanophone : M. Bruno HICK et M. Andreas SCHENK.

1.3 La mission

Le rôle, la mission et les moyens du Collège sont définis dans la loi du 7 février 2014, chapitre 7, article 25, modifié par la loi du 19 avril 2018, dont le texte suit.

« § 1. Lors de l'élection des membres de la Chambre des représentants, du Parlement européen et des Parlements de communauté et de région, ces experts contrôlent la préparation, l'utilisation et le bon fonctionnement de l'ensemble de systèmes de vote, de décryptage, d'enregistrement et de totalisation électroniques ainsi que les procédures concernant la confection, la distribution et l'utilisation des appareils, des logiciels et des supports d'information électroniques. Le Collège d'Experts contrôle également la préparation, l'utilisation et le bon fonctionnement des matériels, logiciels et procédures de transmission et de diffusion digitale des résultats ainsi que tout logiciel utilisé dans le cadre des élections même lorsque le vote se déroule selon d'autres modalités que celles prévues par la présente loi.

Les experts reçoivent du ministre de l'Intérieur ou de son délégué le matériel ainsi que l'ensemble des données, renseignements et informations utiles pour exercer un contrôle sur les systèmes de vote, d'enregistrement et de totalisation électroniques et sur les systèmes de transmission digitale des résultats. Les membres de bureaux électoraux, les organismes d'avis visés à l'article 4, § 3, alinéa 2 et les entreprises privées — ainsi que leurs membres — associées par les autorités compétentes au déroulement du processus électoral fournissent également aux experts le matériel ainsi que l'ensemble des données, renseignements et informations utiles pour exercer le contrôle visé à l'alinéa 1er.

Les experts peuvent notamment émettre dans les bureaux de vote — durant l'élection — des votes qui ne sont ni scannés ni comptabilisés, vérifier la fiabilité des logiciels des systèmes de vote, la transcription exacte des votes émis sur les bulletins de vote, la transcription exacte, par la lecture du code-barres présent sur chaque bulletin de vote, des suffrages exprimés sur le support de mémoire du bureau de vote, l'enregistrement exact du support de mémoire provenant du bureau de vote sur le support de mémoire destiné à la totalisation des votes et la totalisation des suffrages exprimés. Ils peuvent également vérifier la fiabilité des logiciels de transmission digitale des résultats électoraux.

Le Collège d'Experts peut procéder à un audit des résultats afin de garantir la fiabilité et l'intégrité du système de vote électronique avec production d'un bulletin de vote en papier.

Ils effectuent ce contrôle à partir du quarantième jour précédant l'élection, le jour de l'élection et après celle-ci, jusqu'au dépôt du rapport visé au § 2. »

Rapport du Collège d'experts – élections de 2019

1.4 Le rapport

« § 2. Au plus tard quinze jours après la clôture des scrutins et en tout état de cause avant la validation des élections pour ce qui concerne la Chambre des représentants, les Parlements de communauté et de région et le Parlement européen, les experts remettent un rapport au ministre de l'Intérieur ainsi qu'aux assemblées législatives fédérales, régionales et communautaires. »

1.5 Secret

« § 3. Les experts sont tenus au secret. Toute violation de ce secret sera sanctionnée conformément à l'article 458 du Code pénal. »

1.6 Mise à disposition des moyens nécessaires

« § 4. La Chambre des représentants veille à mettre à disposition du Collège d'experts les moyens et ressources nécessaires pour l'accomplissement des tâches visées au présent article. »

2 Législation

Depuis les dernières élections simultanées de 2014, la législation organisant le vote électronique a fait l'objet de quelques modifications reprises ci-dessous.

2.1 Modifications concernant les systèmes de vote

Deux modifications ont été opérées aux systèmes de vote :

- Un système d'obturation automatique de la fente de l'urne a été ajouté afin d'éviter que l'électeur ne place son bulletin de vote dans l'urne avant de l'avoir scanné. La fente s'ouvre automatiquement après que le bulletin ait été scanné et reste ouverte pendant quelques secondes. Elle se referme ensuite pour attendre le prochain vote.
- Pour faciliter le vote des électeurs malvoyants ou aveugles, un des ordinateurs de vote présents dans les bureaux de votes des communes d'Alost et de Malines a été muni d'un boîtier électronique et d'écouteurs permettant à un électeur malvoyant ou aveugle d'exprimer son vote de manière autonome sans utilisation de l'écran de visualisation tactile.

2.2 Modifications concernant la publication des codes sources

Les codes sources sont publiés par le SPF Intérieur dans la semaine qui suit les élections. Ils ne comprennent pas les éléments de sécurité et restent accessibles pendant une période de 6 mois.

2.3 Modifications concernant le Collège d'experts

- Les membres du Collège permanent sont désignés 3 mois avant l'élection du Parlement européen. Ils restent en place tant qu'une nouvelle désignation n'a pas eu lieu.
- Le rôle du Collège d'experts est étendu à tout logiciel utilisé dans le cadre des élections, même lorsque le vote ne se déroule pas électroniquement.
- La Chambre des représentants veille à mettre à disposition du Collège d'experts permanent les moyens et ressources nécessaires à l'accomplissement de ses tâches.
- La Chambre des représentants ou un Parlement de Communauté ou de Région peuvent confier au Collège d'experts permanent des missions spécifiques de contrôle et d'étude relatives à la sécurisation et à la fiabilité des différents systèmes, logiciels et matériels utilisés lors des élections.

3 Description des systèmes

Deux systèmes sont à considérer pour le contrôle du Collège :

1. le système « Martine » développé par la société Civadis, chargé de la collecte des données de base pour l'élection (listes, candidats, intervenants, etc.), la collecte des résultats provenant des bureaux de votes ou des bureaux de dépouillement, le calcul et la diffusion des résultats des élections;
2. le système de vote électronique mis au point par la société SmartMatic et utilisé dans 157 communes de la région flamande, les 19 communes de la région de Bruxelles -Capitale et les 9 communes de la communauté germanophone.

Ces systèmes sont pour l'essentiel identiques à ceux utilisés à l'occasion des élections communales de 2018.

3.1 Description fonctionnelle globale

Avant les élections, le système Martine sert entre autres à récolter les données des candidats pour confectionner les listes. Les fichiers informatiques générés par cette opération sont intégrés à l'environnement de SmartMatic qui sert à la production des clés USB utilisées le jour des élections.

Le jour des élections, à la clôture des opérations dans le bureau de vote, la machine du président génère un fichier résultat « X7S » par élection, qui contient la totalisation des votes émis dans ce bureau.

Au bureau principal, le système Martine injecte ce fichier résultat dans un serveur central qui effectue la totalisation de tous les bureaux par commune et par canton, calcule les résultats complets de l'élection et diffuse les résultats.

Pour le vote traditionnel, dans le bureau de canton, le système Martine sert à l'encodage des résultats des bureaux de dépouillement.

3.2 SmartMatic

3.2.1 Description fonctionnelle

Le système SmartMatic existe en deux versions : la version utilisée pour la première fois en 2012 et une version 2018 utilisée dans les communes qui, à l'occasion des élections de 2018 ou de 2019, ont décidé de passer au vote électronique.

3.2.1.1 L'urne et la machine du président

La version 2012 est constituée d'un ordinateur de type « portable » auquel sont connectés un hub USB muni de deux clés USB identiques, une urne électronique et un lecteur-enregistreur de cartes à puces. Les clés USB contiennent tous les logiciels du bureau de vote, tant pour la machine du président que pour les machines à voter. L'urne est composée d'un réservoir destiné à collecter les votes imprimés par les machines à voter et est coiffée d'un scanner de QR-codes.

Rapport du Collège d'experts – élections de 2019

Dans la version 2018, le PC du président du bureau de vote s'apparente à un PC à écran tactile connecté au hub USB de l'urne qui lui fournit son alimentation.

3.2.1.2 La machine à voter

La machine à voter SmartMatic est un ordinateur basé sur des composants standard placés avec un boîtier particulier muni d'un écran tactile, d'un lecteur de cartes à puce et d'une imprimante intégrée. L'interrupteur, la prise pour le raccordement au réseau électrique, les connecteurs USB, le connecteur pour l'alarme sont situés sur la face arrière. Les seuls composants de l'ordinateur auxquels l'électeur a accès sont le lecteur de carte à puce, l'écran tactile et l'imprimante qui sont sur la face avant. Une machine à voter n'a ni clavier ni disque dur.

Dans deux cantons (Alost et Malines) expérimentant une interface audio pour les malvoyants et les aveugles, les machines à voter disposent en plus d'un boîtier permettant de brancher un casque audio et disposant de touches pour la navigation et la sélection des élections, des listes et des candidats.

À l'occasion des élections, deux versions de la machine à voter sont présentes : la version originale de 2012 et la nouvelle version de 2018. Ces deux versions diffèrent au niveau de la taille de l'appareil, des positions du lecteur de carte à puce et de l'imprimante. Pour le reste, elles offrent les mêmes fonctionnalités.

3.2.2 La procédure électorale avec preuve papier**3.2.2.1 L'ouverture du bureau de vote avec preuve papier**

La première opération consiste à démarrer la machine du président à l'aide des deux clés USB identiques qui lui ont été fournies en même temps que ses mots de passe.

Le président et son bureau vérifient le bon raccordement des différents éléments et démarrent la machine du président. Ensuite vient une phase de diagnostic de la machine du président et des périphériques raccordés (clés USB, urne, valideuse de carte à puce, clavier, souris...).

La machine du président demande de démarrer les machines à voter. Une des clés USB est nécessaire pour démarrer les machines à voter. Lorsque toutes les machines à voter sont prêtes, les clés USB sont réintroduites dans la machine du président.

3.2.2.2 Le déroulement du vote

Le vote est réalisé sur la machine à voter qui se trouve dans l'isoloir. La machine à voter imprime une preuve papier reprenant les votes sous forme lisible ainsi que leurs représentations sous forme de QR-code.

Chaque électeur reçoit une carte à puce initialisée pour lui permettre de voter. Il l'emporte dans l'isoloir et l'introduit dans la machine à voter. Toute carte mal initialisée, non initialisée ou déjà utilisée est refusée. Cette carte ne sert qu'à démarrer l'opération de vote et ne contient aucune autre information ; elle ne sert pas à enregistrer le vote.

L'écran affiche des indications pendant toute l'opération de vote. Il est demandé à l'électeur de choisir la langue de l'interface. Il peut ensuite exprimer ses votes (vote

Rapport du Collège d'experts – élections de 2019

blanc, vote en tête de liste, un ou plusieurs candidats de la même liste) pour chaque élection que le système lui présente. A chaque étape, il lui est demandé de confirmer avant de passer à l'étape suivante. Lorsque l'électeur a confirmé son vote pour une élection sur l'écran tactile, le vote est définitif ; l'électeur ne peut plus le changer. Tant qu'il n'est pas confirmé, l'électeur peut annuler son vote et recommencer.

Après confirmation du vote, la machine à voter imprime le vote sous forme textuelle ainsi que sous la forme d'un QR-code sur un bulletin « preuve papier » et invite l'électeur à retirer la carte à puce. Dans un isoloir prévu à cet effet, l'électeur peut scanner le QR-code de sa preuve papier au moyen d'un scanner à main. Le contenu du QR-code est alors affiché à l'écran et l'électeur peut vérifier son vote.

L'électeur se dirige ensuite vers l'urne où il lui est demandé de placer le QR-code de son bulletin de vote au-dessus du scanner de l'urne. Après confirmation sonore et visuelle que le QR-code a bien été lu et enregistré par l'ordinateur du président, la fente de l'urne s'ouvre et l'électeur introduit son bulletin de vote dans l'urne. Il remet la carte à puce au président ou à un assesseur.

3.2.2.3 La clôture du bureau de vote

A l'issue du scrutin, le bureau de vote est clôturé et un rapport reprenant les chiffres-clés est imprimé. Ce rapport est signé de manière manuscrite par les membres du bureau de vote et joint à leur PV.

L'urne est ouverte et les bulletins « preuves papiers » sont transférés dans une enveloppe. Cette enveloppe contenant les bulletins de vote est ensuite scellée. Le procès-verbal, les clés USB du bureau et l'enveloppe contenant les bulletins de vote sont emmenés au bureau principal.

3.2.3 Éléments techniques du système SmartMatic utilisé dans les bureaux de vote

Le système SmartMatic utilisé dans les bureaux de vote s'exécute à partir des supports mémoires de type clés USB. Ces clés USB contiennent tous les programmes et toutes les données nécessaires au fonctionnement des différents ordinateurs (machine du président et machine de vote) et périphériques (urne et scanner à main présent dans un isoloir).

Les clés USB sont produites de manière centralisée et sont strictement identiques pour tous les bureaux de vote, tant pour la version 2012 que pour la version 2018 du matériel SmartMatic. Elles ne deviennent spécifiques à un bureau de vote qu'après le premier démarrage et l'introduction du nom du bureau et du mot de passe correspondant.

À partir de ce moment, les clés ne peuvent plus être utilisées que pour ce bureau de vote spécifique.

La clé contient par ailleurs deux zones de stockage, appelées « partitions » en jargon informatique : l'une est propre et spécifique aux programmes qui tournent dans le bureau de vote le jour des élections. Dans ce rapport, elle est identifiée en tant que « partition SmartMatic ». L'autre sert au stockage des données et des résultats du bureau de vote qui doivent être transférés à l'environnement Martine pour la

Rapport du Collège d'experts – élections de 2019

totalisation par commune et le calcul des résultats de cette commune. Dans ce rapport, elle est identifiée en tant que « partition Martine ».

3.2.3.1 Partition SmartMatic

À chaque bulletin de vote scanné par l'urne, une copie du vote exprimé est stockée dans un fichier signé et crypté avec extension « .VT » dans le dossier « /SAESLocal/SAES/Votes » de la clé. À la fin de la journée, ce dossier contient autant de fichiers « .VT » qu'il y a eu de bulletins scannés.

Au moment de la clôture des opérations, un fichier « résultat » avec extension « .X7S » est généré pour chaque élection. Ces fichiers sont numériquement signés et cryptés de manière à ne pouvoir être décryptés que par l'application Martine chargée de les totaliser.

3.2.3.2 Partition Martine

À la clôture du bureau de vote, les fichiers « .VT » et « .X7S », ainsi que quelques autres fichiers de contrôle, sont copiés depuis la partition SmartMatic vers la partition Martine.

Parmi les fichiers de contrôle se trouve le fichier PDF qui sert à l'impression dans le bureau de vote du « Rapport des chiffres-clés ».

3.3 Martine

Martine est une plateforme en ligne multitâches, permettant, entre autres, la gestion de la structure de l'élection, du nom et du nombre des bureaux principaux, du nombre de bureaux de vote par commune et de leur adresse, des contacts, des actes de dépôts, des PV d'arrêts, des PV de dépouillement, des résultats de vote.

Les acteurs concernés par Martine sont :

- les communes,
- les bureaux principaux,
- les candidats,
- le pouvoir organisateur.

3.3.1 Infrastructure

La solution repose sur un environnement virtualisé basé sur une distribution Linux Centos/Redhat et VMware ESXi hypervisor. L'application se répartit au minimum sur 3 serveurs. Tous les modules sont déployés de manière redondante selon le principe du mode de fonctionnement « actif/actif ». Les bases de données et le filesystem serveur fonctionnent en mode « actif/passif ».

Au minimum deux lignes redondantes sont disponibles, une en production, l'autre en alerte. Les bases de données principales et de sauvegarde se synchronisent en continu. Les infrastructures sont équipées d'alimentations électriques, de connexions Internet, de switches, firewalls... redondants.

3.3.2 Logiciels

Martine est construite à partir d'ensemble de briques logicielles que l'on peut diviser en trois catégories :

- « Web modules », conçus pour les utilisateurs ;
- « Back end modules », pour gérer en arrière-plan les données et les résultats des candidats ;
- « Support modules » à usage interne pour des tâches spécifiques.

3.3.2.1 Les modules

Martine propose les modules décrits ci-dessous.

3.3.2.1.1 MA1X (Web)

MA1X offre les outils pour préparer les listes électorales.

3.3.2.1.2 MA2X (web)

MA2X est utilisée par l'équipe du bureau principal pour collecter les votes. Pour les bureaux de votes « papiers » les données sont encodées manuellement dans le système. Pour les bureaux de vote électronique, les données de vote sont obtenues via l'introduction de la clé USB SmartMatic. Les fichiers lus (fichiers ".X7S" et ".VT") sont transférés vers MA2X et enregistrés pour des traitements ultérieurs.

MA2X s'occupe également de la production des résultats partiels et définitifs par bureau principal.

3.3.2.1.3 MA3X (web)

MA3X contient les informations relatives aux bureaux de vote et aux bureaux de dépouillement : les adresses et personnes de contacts, le président et le secrétaire du bureau, etc.

MA3X est également utilisé par MA1B (voir ci-dessous) et MA2X pour autoriser l'accès des utilisateurs authentifiés.

3.3.2.1.4 MA1L

MA1L sert à la préparation des actes de dépôt des candidats.

3.3.2.1.5 MA1B (Web)

MA1B va réceptionner les actes de candidatures avant d'aboutir à un procès-verbal d'arrêt définitif avec le détail des listes reçues de MA1X. MA1B enregistre aussi les listes finalisées dans le backend Martine.

3.3.2.1.6 MA3S

MA3S supervise les opérations effectuées dans MA3X par les communes et les bureaux principaux. Les modules « Collect » et « Calcul » permettent de suivre l'arrivée des fichiers sur les serveurs centraux du pouvoir organisateur. Le module « Cockpit » permet de suivre toutes les opérations effectuées par l'ensemble des modules.

Rapport du Collège d'experts – élections de 2019

3.3.2.1.7 DECRYPT (Support)

DECRYPT offre une interface de service à MA2X afin qu'il puisse lire et renvoyer des informations à partir de fichiers de résultats de vote chiffrés. Il est défini en tant que module distinct uniquement pour la sécurité. Il n'est pas accessible à partir d'Internet et peut donc être séparé davantage au niveau du réseau pour optimiser le contrôle d'accès. Le déchiffrement nécessite la clé de déchiffrement privée pour les fichiers lus à partir de clés USB.

3.3.2.1.8 MA1-COLLECT (Backend)

MA1-COLLECT est le point d'entrée principal pour les fichiers générés, avec interface de surveillance. Il effectue une validation simple des fichiers reçus et les stocke pour un traitement ultérieur par MA2-CALCULATE. MA1-COLLECT est également utilisé par MA2X pour lire les données de résultat nécessaires à la production de ses PV finaux.

3.3.2.2 Accès aux modules

L'accès aux modules destinés aux communes, aux bureaux principaux et aux formations politiques est conditionné par l'introduction d'une carte d'identité électronique avec le code pin associé. Ces modules sont : MA3X, MA1L, MA1B, MA2X.

Les utilisateurs des modules MA3X ne sont pas connus avant l'élection par les pouvoirs organisateurs. Ils sont désignés en interne par les communes (MA3C) ou par les présidents des bureaux principaux (MA3B). Un système de SPOC (« single point of contact ») a été mis au point pour permettre l'association d'un bureau avec ses utilisateurs. Martine associe à chaque bureau principal un login/password qui est transmis aux bureaux concernés par la voie officielle mise en place par le pouvoir organisateur.

La personne qui dispose du login/password du bureau peut s'enregistrer dans MA3x en introduisant sa carte d'identité et son code pin. Cette personne devient alors le SPOC principal pour ce bureau et pourra avoir accès par la suite à ce module en utilisant uniquement sa carte d'identité. L'utilisation du login/password n'est nécessaire que pour la première connexion.

Un SPOC peut désigner un SPOC backup dans son bureau.

4 Contrôles et constatations

4.1 Contrôles effectués avant le jour des élections

4.1.1 Contrôles du système SmartMatic

4.1.1.1 Remise du code source et compilation de référence

Une réunion de remise du code source et de compilation de référence a été organisée le 27 février 2019 au SPF Intérieur en présence de l'organisme d'avis, de représentants de la firme SmartMatic et de membres du Collège d'Experts.

Prévue initialement une semaine plus tôt, la réunion avait dû être reportée. En effet, une incompatibilité entre les systèmes SmartMatic et Martine avait été découverte au niveau des modes de calcul de certains éléments de sécurité.

À l'occasion de cette réunion, SmartMatic a présenté les modifications apportées aux systèmes de vote électronique, celles-ci découlant essentiellement de recommandations des Collèges d'experts (fédéral ou régionaux) ou du CCB (Center for Cyber Security Belgium).

- activation des cartes à puces,
- présence d'un clapet de l'urne,
- mise à jour des algorithmes cryptographiques,
- mise à jour des algorithmes d'empreinte digitale (hash code),
- génération automatisée des codes d'initialisation,
- listes des caractères typographiques pouvant être utilisé dans les mots de passe,
- méthode d'introduction du mot de passe,
- police de caractère plus grande pour les noms des partis imprimés sur les billets de vote,
- gestion de l'extraction prématurée des clés USB (suite à l'incident de 2018),
- module audio et permettant la navigation et la sélections des listes et des candidats pour les électeurs mal-voyants,
- impression du rapport du bureau de vote au moyen d'une machine à voter en lieu et place d'un imprimante à jet d'encre,
- partition FAT32 pour le transferts des résultats du bureau de vote.

Certaines étaient déjà implémentées à l'occasion des élections de 2018.

L'application a ensuite été compilée sur un PC vierge. La procédure suivie fut la suivante :

- démarrage du PC de compilation sur une clé USB contenant un système d'exploitation Linux Ubuntu 14.04 LTS ;
- installation d'Ubuntu 14.04 LTS sur le PC de compilation ;
- redémarrage du PC de compilation sous Ubuntu et copie du code source fourni par SmartMatic ;
- compilation et génération de l'image disque de l'environnement ECM (machine de préparation) ;

Rapport du Collège d'experts – élections de 2019

- compilation et génération de l'image disque de la machine président (PM) et de la machine à voter (VM) ;

À la fin de la compilation, une copie du code source et des images disques générées ont été copiées sur différentes clés USB et remise sous enveloppe scellée aux représentants de l'organisme d'avis, du Collège et de SmartMatic.

Une copie a également été mise sous enveloppe scellée pour mise au coffre et une dernière copie, également sous enveloppe scellée, a été laissée au SPF Intérieur pour les étapes suivantes devant aboutir à la confection des clés USB à utiliser le jour des élections.

Enfin, des représentant du SPF Intérieur, du Collège, de l'organisme d'avis et SmartMatic se sont rendus à l'agence bancaire pour la mise au coffre.

4.1.1.2 Rapport de l'organisme d'avis

L'organe consultatif agréé pour les systèmes de vote électronique tels que décrits à l'article 4 § 3 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier pour les élections du Parlement européen, de la Chambre des représentants et des Parlements de communauté et de région dans les communes où il est fait usage d'un système de vote électronique avec preuve papier est la société PricewaterhouseCoopers (PwC).

La société PwC a été mandatée pour la vérification de l'adéquation des applications du système SmartMatic (convention PwC-SmartMatic du 23 janvier 2019).

À l'occasion d'une réunion organisée le 21 mars 2019, l'organisme d'avis PwC a présenté un pré-rapport de son analyse du système de vote SmartMatic. Cette approche en plusieurs phases était indispensable afin de pouvoir tester la compatibilité entre SmartMatic et Martine au niveau des échanges de données, tous les modules de Martine n'étant pas encore terminés.

L'analyse s'est focalisée sur l'application de préparation du système de vote, y compris le système de duplication, le système du président de bureau, l'urne, les machines à voter et l'application de recomptage. PwC a réalisé de multiples contrôles automatisés et a conduit des entrevues avec l'équipe en charge du développement.

L'avis définitif a été remis le 12 avril 2019.

Les experts ont reçu copie de l'avis définitif de l'organisme d'avis le 14 avril 2019.

Cet avis mentionne toute une série de problèmes qualifiés de « non-bloquants » et pouvant être neutralisés par des procédures ou des interventions manuelles, notamment au niveau de l'application de préparation du système de vote et d'injection des listes électorales et des listes de candidats.

4.1.1.3 Inclusion d'un correctif suite à un problème détecté par le SPF intérieur avant le pré-rapport de l'organisme d'avis

Le 15 mars 2019, soit une semaine avant le pré-rapport de l'organisme d'avis, le SPF intérieur a découvert et signalé un problème au niveau des machines président de première génération. Ces machines sont équipées de souris qui n'étaient pas

Rapport du Collège d'experts – élections de 2019

reconnues par le système, SmartMatic ayant oublié de les inclure dans le fichier de configuration des périphériques pouvant être raccordés au système.

La solution au problème consistait donc à ajouter dans un fichier de configuration de la machine président, l'information permettant à celle-ci de reconnaître la souris et de l'accepter comme périphérique autorisé.

La société SmartMatic a proposé une solution technique au SPF Intérieur qui l'a soumise au Collège. Celui-ci a émis un avis négatif par rapport à la proposition faite, estimant que celle-ci et sa mise en œuvre s'écartait de manière significative et inutile de la procédure habituelle de génération de la clé USB « maître ». Il a dès lors été décidé de corriger le problème au niveau de l'image disque de la machine du président et de corriger manuellement le fichier de configuration des périphériques.

Le 25 mars 2019, en présence de représentants du SPF Intérieur, du Collège d'experts et de l'organisme d'avis, les représentants de la société SmartMatic ont corrigé l'image disque de la machine président en incluant le correctif requis au niveau du fichier de configuration des périphériques. Cette opération a été effectuée sur le PC de compilation et chaque partie a reçu une nouvelle copie de l'environnement de compilation (copie des images disque pour l'environnement de préparation, pour la machine président et pour la machine à voter).

4.1.1.4 Création de l'environnement de préparation ECM

Comme évoqué plus haut, l'environnement SmartMatic comporte un environnement de préparation de la clé USB de base dont des copies seront utilisées dans tous les bureaux de vote le jour des élections. Cet environnement de préparation comporte deux serveurs et un PC client, tous les trois raccordés sur un réseau isolé.

L'image disque « ECM » générée lors la compilation sert à installer et configurer ce PC et ces deux serveurs.

Le 15 avril 2019, dans les locaux du SPF Intérieur, cet environnement de préparation de la clé USB de base, appelée « clé master », a été installé et démarré par les représentants du SPF Intérieur en présence de membres du Collège et de représentants de la société SmartMatic.

La liste des bureaux de votes a été chargée dans l'environnement « ECM » et les différents éléments cryptographiques nécessaires aux élections ont été générés. Le Collège en a pris une copie.

4.1.1.5 Génération des impressions d'écrans

À la suite de la clôture des candidatures enregistrées au moyen de Martine, les jeux de données contenant les listes électorales et les listes de candidats ont été chargés dans l'environnement de préparation (« ECM »).

Ceci s'est fait en présence du Collège, le 24 avril 2019.

À partir de cet environnement est alors générée une clé USB particulière qui est utilisée sur une machine à voter pour générer des captures d'écrans des listes et candidats. Ces captures d'écrans sont ensuite soumises à l'approbation des présidents des bureaux principaux.

Rapport du Collège d'experts – élections de 2019

4.1.1.6 Génération de la « clé master » pour les élections

Lors de l'approbation plus d'une centaine de corrections ont encore été demandées par les présidents des bureaux principaux pour corriger des erreurs qu'ils auraient dû détecter bien avant.

Le risque d'erreur est réel. En effet, à ce stade de préparation des élections, procéder de la sorte implique de devoir introduire deux fois toutes ces corrections, une fois dans l'environnement SmartMatic et une fois dans l'environnement Martine.

Suite à ces corrections, le pouvoir organisateur a pu générer la « clé master » et sa duplication sur plus de 9000 clés USB.

Le Collège a pris une copie de la « clé master » afin de l'utiliser comme référence pour ces contrôles après les élections.

4.1.1.7 Confection des supports mémoire

Le 10 mai 2019, le Collège a visité les locaux où les supports informatiques utilisés pour les élections ont été dupliqués. Il s'agit des clés USB et des enveloppes contenant les mots de passe. Le couloir reprenant tous les locaux de confection est sécurisé via un système de badge, un garde et des caméras. Les locaux individuels sont fermés à clé. Le personnel chargé de la copie des clés USB et de l'impression des mots de passe est du personnel propre au SPF Intérieur.

4.1.1.8 Environnement de test du Collège

Le Collège s'est doté d'un environnement de test, composé de machines virtuelles pour l'environnement « ECM » et a généré sa propre « clé master » qu'il a dupliqué à une vingtaine d'exemplaires en vue d'effectuer des tests portant sur différents cantons. Pour cela, le Collège dispose d'une machine de président et d'une machine à voter de la génération 2018 avec lesquelles il a effectué les opérations suivantes :

- ouverture d'un bureau de vote (démarrage urne et machine du président) ;
- démarrage de machines à voter ;
- émission de votes et visualisation de votes sur l'ordinateur de vote ;
- décryptage des fichiers « .VT » à l'aide d'un logiciel du Collège et comparaison avec la version lisible du vote.

Tous ces tests se sont avérés concluants sur le plan logiciel.

C'est lors de ces tests que le Collège a découvert une discordance dans les versions linguistiques du logiciel de la machine à voter. En effet, dans les versions française et allemande apparaît en fin de vote un message invitant l'électeur à vérifier son vote à l'aide du scanner à main prévu à cet effet dans un isoloir séparé. Dans la version néerlandaise, ce message n'apparaît pas.

Le Collège en a averti le SPF Intérieur dès sa découverte. Celui-ci n'avait pas détecté ce problème et l'organisme d'avis non plus. Malheureusement, vu le caractère tardif de cette découverte, il n'a pas été possible d'y remédier, les clés USB ayant déjà été générées et mises sous enveloppe.

Rapport du Collège d'experts – élections de 2019

Interrogé à ce sujet, le SPF Intérieur a communiqué oralement que l'origine de ce problème se situait dans les fichiers sources fournis par SmartMatic qui s'est visiblement inspiré des fichiers de configuration utilisés à l'occasion des élections communales et provinciales en Flandre en 2018. En effet, le pouvoir organisateur de ces élections en Flandre ne souhaitait pas voir cette mention invitant le citoyen à un contrôle supplémentaire.

4.1.2 Contrôle du système Martine – module MA2X

La société PwC s'est vu confier le mandat de vérifier l'adéquation du système Martine (accord PwC-Civadis du 26 février 2019). L'analyse était limitée au module MA2X et concernait (1) la sécurité, l'intégrité, la fraude et le secret de la procédure électorale, (2) le respect de la législation, (3) le caractère fonctionnel et résilient des systèmes. PwC a effectué de nombreux contrôles automatisés et a eu des entretiens avec l'équipe de développement.

Le 17 mai 2019, le collège a assisté à la présentation du rapport de PwC sur son évaluation de MA2X (module de traitement des résultats de Martine). À ce moment-là, le Collège avait également reçu le rapport de langue française de PwC concernant MA2X.

En ce qui concerne les autres constatations, il est apparu au cours de la présentation que sur un nombre important d'entre elles, les sociétés PwC d'une part et, le fournisseur CIVADIS d'autre part, avaient de grosses divergences d'opinion sur leur interprétation correcte. Au cours de la réunion, il a été convenu d'offrir à CIVADIS la possibilité de répondre par écrit. Cette réponse serait traitée ou ajoutée au rapport d'évaluation de PwC pour arriver à une version finale.

Au moment de l'édition de son rapport, le Collège n'avait pas encore reçu ce document mis à jour.

Les commentaires suivants peuvent être formulés à propos du rapport de PwC:

- PwC n'a pas étudié un certain nombre d'aspects du système. (pages 11-12 de leur rapport). Cela inclut les systèmes utilisés dans les bureaux principaux pour lire les clés USB et / ou pour envoyer les votes comptés manuellement à la base de données centrale de Bruxelles. Comme l'expérience l'a montré, un certain nombre de ces éléments sont en effet importants pour, par exemple, la fiabilité et la convivialité du système.
- Il a été constaté que jusque peu avant les élections, des modifications avaient été apportées au logiciel (dernière version le 9 mai). Cela rend impossible une analyse approfondie du logiciel, tel que prévue dans la loi électorale.

En fin de compte, PwC a donné l'avis suivant: «Sur la base des travaux que nous avons effectués et à condition que les instructions (supplémentaires) et / ou les procédures manuelles (supplémentaires) nécessaires soient mises en œuvre et exécutées, et en vous référant à la définition de l'aptitude, les décisions prises nous avons l'assurance

Rapport du Collège d'experts – élections de 2019

raisonnable¹ - mais pas absolue - que l'application "Gestion des résultats" (MA2X) répond aux critères d'adéquation définis ci-dessus "

4.1.3 Relations entre les firmes responsables des développements

Afin de garantir l'authenticité et la fiabilité des données qui sont échangées entre les systèmes SmartMatic et Martine (développé par Civadis), données nécessaires à la création des clés USB et au calcul des résultats, différents mécanismes techniques informatiques sont mis en œuvre :

- Encryption
- Signature électronique
- Calcul d'empreinte numérique (hash code)
- Somme de contrôle (checksum)
- Etc.

La compatibilité des deux systèmes est donc indispensable et une bonne coordination entre les deux firmes responsables des développements logiciels sont essentielles. Le SPF Intérieur a informé le Collège de ce que plusieurs incidents de parcours ont émaillé la préparation des élections, les sociétés SmartMatic et Civadis (développeur de Martine) se rejetant régulièrement la responsabilité lors de problèmes de compatibilité ou d'interprétation des normes, standards et conventions à implémenter dans leurs logiciels.

Le Collège regrette vivement ce manque de collaboration entre SmartMatic et Civadis.

4.1.4 Analyse des codes sources

Le Collège d'experts a analysé succinctement, étant donné la courte durée de sa mission, la manière dont la sécurité informatique est mise en œuvre dans les différents systèmes, sur base du code source et des documents techniques reçus des entreprises. Le Collège d'experts émet dans ce rapport une série de recommandations relatives à la sécurité des systèmes de vote et à la mise en œuvre des techniques cryptographiques.

Le Collège d'experts suggère aussi des mesures (sur base de réalisations systématiques d'audits, de relectures systématiques des votes par les électeurs, de normes de qualité des codes sources et de la documentation) afin d'améliorer la transparence et la sécurité du processus électoral dans son ensemble, y compris au cours de la période précédant l'élection (développement du code source, génération et gestion des clés cryptographiques).

Le Collège d'experts constate qu'il a parfois été difficile d'obtenir des réponses aux questions posées à la société SmartMatic.

¹ En ce qui concerne le terme « certitude raisonnable » il est référé à l' Arrête royal du 26 mai 2002 relatif au système de contrôle interne au sein des services publics fédéraux (MB 31 mai 2002)

4.1.5 Analyse du CCB

4.1.5.1 Périmètre et méthodologie

Le Collège d'experts a pu rencontrer des spécialistes du Centre pour la Cybersécurité Belgique (CCB) et consulter les différents rapports rédigés par le Centre.

L'approche du CCB s'est concentrée sur plusieurs éléments :

- la gestion de la sécurité au niveau processus ;
- la sécurité du cycle de développement ;
- des recommandations et le suivi de celles-ci ;
- un exercice de pénétration du système de vote (pentesting).

En pratique, ces analyses ont été menées sous forme d'interview, en interaction constante avec les sociétés chargées de développer le système de vote (Civadis et SmartMatic), et/ou en parallèle de manière indépendante. La maturité organisationnelle des sociétés est également évaluée. Les résultats ont été présentés et classés selon, la vraisemblance du risque, sa difficulté de mise en œuvre et enfin l'impact sur les élections. De nombreuses corrections ont été demandées à Civadis et toutes les demandes ont été rencontrées.

Par rapport à l'analyse menée en 2018, un effort important a été fourni pour sensibiliser les responsables techniques des partis politiques à la cybersécurité de leurs installations (sites webs, moyens de communication) et crise.

Le CCB a également aidé à la mise en place d'un DRP (disaster recovery plan) et de procédures formelles pour les incidents envisagés.

A la suite de ces analyses et exercices, le CCB conclut que le processus peut être amélioré mais que le niveau de sécurité de l'ensemble est suffisant pour organiser les élections dans de bonnes conditions.

4.1.5.2 Cycle de développement et gestion de la sécurité

Le CCB a conduit une série d'interviews et a analysé les documents fournis par les sociétés SmartMatic et Civadis.

Globalement, le Collège d'experts constate que le CCB a identifié des vulnérabilités qui auraient pu être identifiées et corrigées par les entreprises avant de la mise en production.

4.1.5.3 Sécurité des machines à voter et de l'application de comptabilisation « Martine »

Lors de cette phase d'analyse, le CCB a procédé à des essais d'attaques du système (en mode dit « purple team »). Le CCB a relevé un certain nombre de points d'attention. Ils ont été transmis aux deux sous-traitants afin qu'ils puissent proposer des correctifs. Une réunion a ensuite eu lieu afin de passer en revue les actions qui avaient été prises.

Rapport du Collège d'experts – élections de 2019

4.1.6 Visite du Datacenter au SPF Intérieur

Les membres du Collège ont visité le centre de données de Martine le 9/5/2019. Les serveurs sont situés dans la salle des serveurs du SPF Intérieur.

Le collège a pu constater que toutes les bonnes pratiques propres aux datacenters sont appliquées :

- sécurité des personnes (accès restreints et contrôlés)
- réseaux (protégés et redondants)
- alimentation électrique (séparée et redondante)
- base de données (dupliquée en temps réel et sauvegardée sur 3 sites)

4.1.7 Participation aux séances de formation**4.1.7.1 Formations des formateurs**

L'objectif était de former le personnel communal, chargé à son tour de former les présidents et secrétaires des bureaux de vote, commune par commune. Etant donné que les formations des formateurs ont eu lieu en décembre 2018 et janvier 2019 et que le Collège permanent n'en a pas été informé, le Collège n'a pas pu assister à ces formations.

4.1.7.2 Formations des présidents de bureaux de vote

Les membres du collège ont assisté aux formations des présidents et secrétaires de bureaux de vote des communes suivantes :

- Alost
- Anderlecht
- Berchem- Saint-Agathe
- Berlare
- Bruxelles
- Eupen
- Lochristi
- Liedekerke
- Lubbeek
- Saint-Josse-ten-Noode
- Saint-Vith
- Woluwe-Saint-Lambert
- Woluwe-Saint-Pierre
- Zele

Globalement, Le Collège a constaté que les formations étaient d'un excellent niveau. Quelques remarques s'imposent cependant :

- la partie clôture du bureau avec les procédures et les formulaires à remplir n'a pas été toujours été expliquée. Par conséquent beaucoup de bureaux de vote ont eu de grandes difficultés pour remplir les formulaires (Berlare, Zele) ;
- il n'y avait pas toujours de matériel de démonstration (Saint-Vith). La fourniture des machines de démonstration aurait créé des coûts qui n'ont pas été prévu dans leur budget ;

Rapport du Collège d'experts – élections de 2019

- certaines communes ont produit leur propre documentation (Berlare) ;
- certaines machines de démonstrations présentaient des problèmes (Aalst, Lochristi) ;
- il est clairement dit (et répété) que si à 7h30, le bureau n'est pas constitué, il faut lancer les PC quand même (Anderlecht, Berchem Saint Agathe , Eupen), ce qui est contraire à la législation qui demandent d'attendre que le bureau soit constitué ;
- certaines salles ne sont pas adaptées : pas de micro, pas suffisamment de bancs pour noter (Anderlecht, Berchem Saint Agathe) ;
- il est parfois conseillé de ne pas faire de publicité pour le scanner à main permettant de contrôler son vote (Bruxelles).
- Le matériel de démonstration était parfois présent mais les présidents de bureaux de vote n'étaient pas invités à le tester (Saint-Josse).
- Lors des formations il n'a pas toujours été mentionner la façon correcte de débrancher les clés USB des machines des présidents.

4.1.8 Respect des procédures

4.1.8.1 Lors de l'installation de l'environnement ECM

A l'occasion de l'installation de l'environnement ECM (cf. 4.1.1.4), le Collège a été très étonné de découvrir que certains fichiers de configuration des élections n'étaient remis au SPF Intérieur qu'à ce moment et qu'ils n'étaient pas présents dans le code source remis par SmartMatic à l'occasion de la compilation de référence. Par ailleurs, certains de ces fichiers ont par la suite dû être modifiés pour corriger quelques problèmes soulevés par le SPF Intérieur et qui n'avaient pas été détectés par l'organisme d'avis et/ou considérés comme non-bloquants.

Ces fichiers ont été soumis à l'organisme d'avis pour aval.

Le Collège déplore qu'il y ait une telle discordance au niveau des procédures entre le formalisme de la compilation de référence (avec copie en présence de témoins, mise sous enveloppes scellées, mise au coffre, etc.) et la remise de manière informelle par la société SmartMatic de certains éléments de configuration et même de programmation, qui ont une incidence sur le fonctionnement de la machine du président et le comportement de la machine à voter.

4.1.8.2 Après la clôture du dépôt des candidatures

Il a été rapporté au Collège que, bien que les listes aient été finalisées et validées par les présidents des bureaux principaux, certains ont encore constaté des erreurs dans celles-ci après leur signature formelle. Ces présidents ont alors exigé de pouvoir apporter des corrections à ces listes sans respecter la procédure imposée par la législation.

Il s'agit d'une centaine de modifications (orthographe des noms des candidats comme l'utilisation de caractères accentués ou non, noms des listes ...).

À Anvers la liste 'Piratenpartij' (liste 23) manquait dans le système Martine. Le parti avait bien déposé sa liste, comme la procédure le prévoit mais elle avait été oubliée.

Rapport du Collège d'experts – élections de 2019

Un PV pour ce problème a été rédigé, et les données manquantes ont été ajoutées dans le tableau final de Martine.

Vu les limites de temps pour la confection des supports mémoire, ces exigences de dernière minute ont contraint les services du SPF INTÉRIEUR à opérer dans l'urgence ces modifications en dehors de la procédure et des dispositions légales, ce qui a pu être la cause d'erreurs.

4.2 Constatations le jour des élections

Le jour du scrutin, les membres du Collège ont procédé à des contrôles dans les bureaux de votes et dans les bureaux de totalisation.

4.2.1 Contrôles dans les bureaux de vote

Les experts ont effectué des contrôles dans un certain nombre de bureaux de vote électronique. Les contrôles ont été principalement de trois types : émission de votes de tests pour analyse ultérieure, réponse à un questionnaire-type, observation du déroulement des opérations.

4.2.1.1 Votes de test

Dans chaque bureau de vote contrôlé, des votes de test ont été émis par les experts du Collège, souvent en présence d'un assesseur désigné par le président du bureau de vote. Les votes émis ont été contrôlés dans l'isoloir prévu pour la visualisation du vote conjointement par l'assesseur et l'expert. Tous les votes ont été fidèlement reproduits à l'écran.

Les bulletins ont ensuite été emportés par l'expert pour être analysés dans un environnement propre au Collège après le jour de l'élection.

4.2.1.2 Questionnaire

Un rapport basé sur un questionnaire-type a ensuite été établi par l'expert avec la collaboration du président du bureau de vote. Les incidents éventuels y ont été consignés. Ce rapport a été établi afin de pouvoir identifier les difficultés rencontrées et de proposer des recommandations en conséquence.

4.2.1.3 Bureaux de vote contrôlés

Les bureaux de vote qui ont été contrôlés sont repris dans le tableau ci-dessous.

Canton	Commune	Bureaux de vote
Aalst	Aalst	5,6,8,61,65
Aalter	Aalter	1,4,5,14
Asse	Affligem	28,31
Saint-Vith	Amblève	11,12,13,14
Hoogstraten	Baerle-Duc	16
Zelev	Berlare	18
Bilzen	Bilzen	16
Puurs-Saint-Amands	Bornem	14
Bruxelles	Bruxelles	12,13,15,25,26,28,29

Rapport du Collège d'experts – élections de 2019

Canton	Commune	Bureaux de vote
Saint-Vith	Bullange	16,17,18
Saint-Vith	Burg Reuland	19,20,21
Saint-Vith	Bütgenbach	22,23,24,25,27
Deinze	Deinze	1,3
Asse	Dilbeek-Schepdaal	45,68
Bruges	Dudzele	112
Saint-Vith	Elsenborn	22
Ixelles	Ixelles	4,13,48,51
Saint-Josse-Ten-Noode	Etterbeek	13,17,24
Eupen	Eupen	1,3,8,9,10
Lennik	Gaasbeek	4
Molenbeek-Saint-Jean	Ganshoren	55
Léau	Geetbets	12,14
Glabbeek	Glabbeek	5
Hasselt	Hasselt	8,11,57,58
Louvain	Herent	95
Molenbeek-Saint-Jean	Jette	73, 82
Kalmthout	Kalmthout	45
Eupen	Kelmis	17,18,19,20
Bruges	Knokke-Heist	182
Molenbeek-Saint-Jean	Koekelberg	104
Furnes	Coxyde	42
Courtrai	Courtrai	17,18,20,55,61
Rhode-St-Genese	Krainem	26
Lennik	Lennik-Gaasbeek	8
Louvain	Louvain	2,11,160,78,69
Léau	Linter	24
Lochristi	Lochristi	11
Eupen	Lontzen	21,23,24,25
Ostende	Ostende	64
Ixelles	Auderghem	57, 62, 77
Eupen	Raeren	27,29,30
Roulers	Roulers	42, 44
Saint-Gilles	Saint-Gilles	18
Saint-Vith	Saint-Vith	5,6,7,8
Schaerbeek	Schaerbeek	62
Anderlecht	Berchem-Sainte-Agathe	78
Molenbeek-Saint-Jean	Molenbeek-Saint-Jean	21,43
Saint-Josse-Ten-Noode	Saint-Josse-Ten-Noode	1,2,3,9,10,11,12
Saint-Josse-Ten-Noode	Woluwe-Saint-Lambert	67
Saint-Trond	Saint-Trond	17,18,20
Asse	Ternat	115
Tongres	Tongres	22
Furnes	Furnes	7
Fourons	Fourons	1
Ixelles	Watermael-Boitsfort	94,95, 96?

Rapport du Collège d'experts – élections de 2019

Canton	Commune	Bureaux de vote
Rhode-Saint-Genèse	Wemmel	45
Rhode-Saint-Genèse	Wezembeek	54
Saint-Josse-Ten-Noode	Woluwe-Saint-Pierre	99
Léau	Léau	3,9

4.2.2 Incidents dans les bureaux de vote

4.2.2.1 Procédures

4.2.2.1.1 Divers

Description

- ouverture des enveloppes des mots de passe et clés USB avant la constitution complète du bureau ;
- volet protégeant les ports USB dans les machines de vote et urne non scellé ;
- pas de contrôle des votes de test par le lecteur QR dans l'isoloir ;
- enveloppes contenant les clés USB et les codes mises dans le local de vote ;
- absence de votes de test.

Solution

Suivre les instructions du manuel.

4.2.2.1.2 Clés USB connecté à la machine du président

Description

Lors du contrôle du bureau de vote, on a constaté que les clés USB n'étaient pas connectées à l'urne, mais connectées à la machine du président.

Solution

On a éjecté correctement d'abord une clé USB et on l'a connectée à l'urne. Ensuite on a éjecté la deuxième clé USB correctement et le président a également connecté cette clé USB à l'urne.

Dans les configurations « machines président et urnes qui y sont raccordées », le Collège a vérifié que tous les ports USB sont interchangeables et n'influence pas le bon fonctionnement du système.

4.2.2.1.3 Problème de traduction spécifique pour les élections dans la Communauté germanophone

La traduction en allemand des documents « ACEG/11bis » et « Instructions pour les présidents des bureaux de vote utilisant le vote électronique avec preuve papier » ne tiennent pas compte des 4 élections dans les cantons germanophones.

Le procès-verbal en langue allemande créé par MA2X n'a pas été adapté au système de vote électronique actuelle. Il fait, par exemple, encore référence à des disquettes.

4.2.2.2 Matériels

4.2.2.2.1 Exemples

Florilège de problèmes techniques rencontrés :

Rapport du Collège d'experts – élections de 2019

- clés USB non fonctionnelles ;
- problème au démarrage de la machine du président ;
- redémarrage après clés USB en panne ;
- difficultés pour sortir des clés USB de la machine de vote ;
- mauvais fonctionnement de l'écran tactile d'une machine de vote ;
- panne de machine de vote ;
- panne de machine du président ;
- panne d'imprimante ;
- problèmes avec l'impression des preuves papier ;
- problème de lecture des preuves papier par l'urne.

4.2.2.2.2 Solution

En cas de problème avec le matériel des bureaux de vote, la société SmartMatic est contractuellement chargée de remplacer le matériel défectueux dans un délai défini selon le type de panne. Les clés USB de remplacement ont été livrées dans le délai fixé à 30 minutes pour les points qui bloquent les opérations de vote, ce qui était le cas.

4.2.2.3 Autres**4.2.2.3.1 Dysfonctionnement de l'imprimante des machines à voter et double vote****Description**

Des bulletins sont restés bloqués dans l'imprimante de certaines machines à voter. Les électeurs concernés par ce problème ont pu voter à nouveau dans un autre isoloir.

Lors de l'intervention du technicien, le bulletin -- ou les bulletins attachés les uns aux autres -- ont été retrouvés à l'intérieur de la machine à voter. Ce ou ces bulletins ont été parfois erronément scannés et placés dans l'urne par un membre du bureau, enregistrant ainsi un deuxième vote pour les électeurs concernés (Saint-Gilles 18).

Solution

Il faut donner instruction aux bureaux de vote de ne jamais scanner les bulletins bloqués dans les machines à voter sans quoi cela donnerait lieu à un double vote. Ces bulletins doivent être considérés comme nuls et traités comme tels.

4.2.2.3.2 Bulletins placés dans l'urne sans avoir été scannés**Description**

Il est apparu, lors de recomptages d'urne dans les bureaux principaux, que le nombre de votes scannés était supérieur à celui indiqué sur le rapport des chiffres-clés du bureau de vote. Après analyse, la seule explication plausible est que certains bulletins de vote ont été placés dans l'urne sans être scannés.

4.2.3 Contrôles dans les bureaux principaux

Les membres du Collège se sont rendus dans les bureaux principaux suivants le soir des élections :

- Anvers
- Berchem Saint-Agathe

Rapport du Collège d'experts – élections de 2019

- Bruxelles
- Eupen
- Louvain
- Lennik
- Malmedy
- Saint-Gilles
- Saint-Vith
- Tongres
- Zaventem

Une majorité de PC des bureaux principaux ont connu des problèmes de connexion à l'environnement Martine (cf. 4.2.5). Le helpdesk était difficilement joignable.

Ce problème mis à part, les experts ont pu constater que certaines libertés ont été prises lors de l'acheminement des clés USB aux bureaux de cantons (enveloppes parfois non signées, parfois non scellées, parfois même sans emballage)

De même, il a dû être procédé à des recomptages d'urnes dans les bureaux principaux, avec pour seule conséquence une certaine perte de temps.

4.2.4 Incident : Publication prématurée des résultats sur les sites Web des médias

Constatation

Le jour du scrutin, vers 15 h 30, les premiers résultats (un bureau de Tongres) ont été publiés sur le site web de la VRT alors que les élections étaient encore en cours.

Des membres du Collège se sont rendus au bureau concerné où ils ont constaté que les résultats publiés étaient conformes à ceux du comptage manuel. Les discussions avec les membres du bureau de vote, et en particulier avec le président, ont permis de conclure que:

- les résultats n'avaient pas encore été saisis dans Martine ;
- le bureau de vote avait reçu la visite de journalistes.

Un responsable du SPF Intérieur a indiqué qu'aucun résultat n'avait été transmis via Martine, ce qui a été confirmé par le site Internet du SPF Intérieur où aucun résultat n'était affiché.

Il a également été établi que le système Martine n'avait pas envoyé de résultats aux médias avant 16h40.

Conclusion

La diffusion prématurée des résultats du premier bureau à Tongres a été effectuée en dehors des canaux officiels par des journalistes sur place et ne relève pas de la compétence du Collège.

La confirmation par le SPF Intérieur qu'aucun résultat n'avait été diffusé avant 16 heures (également vérifié via le serveur sftp du collège) suggère que les autres

Rapport du Collège d'experts – élections de 2019

résultats publiés par anticipation ont également été obtenus en dehors des canaux officiels.

4.2.5 Incident de la transmission des résultats à partir des cantons le soir des élections

4.2.5.1 Résumé et impact sur le résultat des élections

La procédure de vote prévoit l'envoi des résultats électroniques (contenus sur les clés USB des machines président ou encodées à la main dans le cas du vote papier) depuis les bureaux principaux vers le système Martine.

Peu de temps après l'envoi des premières données, il est apparu qu'une grande majorité des bureaux de canton n'arrivaient plus à se connecter pour s'identifier. Le système a été indisponible pendant plusieurs heures (de 16h à 20h10).

Après analyse des informations transmises au Collège, il a pu conclure que cet incident n'a pas eu d'impact sur les résultats.

4.2.5.2 Description technique des incidents sur base des informations transmises au Collège

4.2.5.2.1 Incident 1 - Accès impossible à l'environnement d'envoi des données depuis les bureaux de votes

L'incident a débuté aux alentours de 16h. Plusieurs bureaux ont téléphoné au helpdesk de Civadis pour signaler l'impossibilité de se connecter aux modules MA2X. Les modules firewall, load-balancer et bases de données continuaient à répondre correctement et les paramètres de charge étaient normaux. Cependant, il n'était pas possible d'établir de nouvelles connexions vers les systèmes. Après analyse des différents éléments (réseau et routeurs Proximus, règles de firewall, etc...), il a été constaté qu'un nombre important de sessions DNS étaient ouvertes sur le firewall de Martine. Ces sessions étaient dues au serveur DNS (privé) utilisé par les clients, et qui a été configuré pour empêcher la résolution des noms autres que ceux autorisés pour Martine. Il s'agit, selon les premières analyses, de vérifications massives de mise à jour de l'environnement Windows 7 provenant des machines mises à disposition des bureaux principaux par Civadis pour encoder et transmettre les résultats des votes, et des routeurs fournis pour l'occasion.

La décision a été prise de rediriger les requêtes DNS traitées par l'infrastructure Martine vers les serveurs DNS du SPF Intérieur. Les sessions ouvertes se sont résorbées aussitôt.

4.2.5.2.2 Incident 2 – Perte de connectivité via le réseau Publilink

Après la résolution de l'incident 1, des problèmes d'accès subsistaient. De nouvelles sessions ne pouvaient être initiées et les sessions perdues ne pouvaient être rétablies.

Après analyse, il apparaît que la connectivité réseau via le réseau Publilink ne permettait pas d'atteindre correctement les serveurs de Martine alors que c'était possible depuis l'Internet ou le réseau du SPF Intérieur. Le support Martine a alors proposé le basculement de l'accès au module MA2X de Publilink vers Internet/Fedman

Rapport du Collège d'experts – élections de 2019

(sur le réseau BELNET). La solution a été validée, en terme de sécurité, par les ingénieurs du CCB et du CERT présents au SPF Intérieur.

A ce moment-là, la connectivité fut rétablie et l'envoi des résultats reprit normalement.

4.2.5.2.3 Incident 3 – filtrage bloquant sur le firewall du SPF Intérieur

En fin de soirée, un ajout de règle filtrage sur le firewall du SPF Intérieur a déconnecté les utilisateurs actifs, amenant un grand nombre d'appels au helpdesk. La règle a été supprimée et les opérations ont pu reprendre normalement.

4.2.5.2.4 Suivi des incidents et conclusion

Le lundi 27, le Collège a demandé au directeur général du SPF Intérieur une analyse complète des événements survenus la veille, un suivi des décisions prises lors des réunions de crise et de consigner les logs des différents intervenants pour analyse ultérieure. Le SPF Intérieur a lancé une enquête interne et a pleinement collaboré avec le Collège, en totale transparence et avec rapidité.

Le Collège a pu conclure, au vu des informations qu'il a reçues et des analyses qu'il a conduites, que les problèmes informatiques n'ont provoqué que des ralentissements du processus. Les propriétés cryptographiques (intégrité des résultats de vote, authenticité des sources d'envoi dans Martine, confidentialité des communications) ont été garanties tout au long du processus. Elles sont conformes à ce qui est attendu du système de vote électronique et d'envoi des données dans Martine.

Le Collège a pu également analyser les plans de DRP (disaster recovery plan), les procédures de gestion de crise et les analyses techniques du CERT / CCB.

4.3 Contrôles effectués après le jour des élections

4.3.1 Vérification des totalisations

Comme à l'occasion des élections de 2014, et en particulier suite aux problèmes détectés lors des élections de 2018², le Collège a à nouveau souhaité procéder à une retotalisation complète des votes contenus dans les supports mémoires utilisés dans les bureaux de vote.

L'objectif était de comparer les résultats obtenus par le Collège au moyen de ses propres logiciels avec les données diffusées par Martine aux médias le soir des élections et également utilisées pour diffuser les résultats sur le site web officiel des élections <https://elections2019.belgium.be/>.

4.3.1.1 Récupération des clés USB

Afin de pouvoir procéder à la retotalisation, le collège devait récupérer toutes les clés USB utilisées le jour des élections. À cette fin, le SPF Intérieur a envoyé une directive à tous les bureaux de canton où est utilisé le vote électronique leur demandant de

² Dans une commune bruxelloise et une demi-douzaine de communes flamandes, une erreur humaine de manipulation avait perturbé la clôture du système de vote, avec comme conséquence que tous les bulletins de vote n'avaient pas été comptés !

Rapport du Collège d'experts – élections de 2019

regrouper toutes les clés USB aux bureaux principaux de circonscription A (pour la Chambre) pour le lundi 27 mai avant 15h.

Malheureusement, cette directive n'a pas été lue par tous les présidents de canton. De plus, dans certains cantons, aucune procédure n'avait été mise en place pour récolter les clés USB. Il n'a pas été possible de récupérer toutes les clés. Au final, il manque 3 jeux de clés répartis sur 3 cantons différents.

4.3.1.2 Lecture des clés USB

Le Collège a mis au point un environnement informatique spécifique (système d'exploitation, logiciel) pour prendre une copie des supports mémoire utilisés dans les bureaux de vote en vue de leur analyse et de leur exploitation.

Au moyen de cet environnement, le Collège a procédé à la prise de copies de toutes les clés USB utilisées dans les bureaux principaux pour la totalisation. Il a également pris des copies des clés USB utilisées pour différents recomptages dans différentes communes. Ces recomptages avaient été décidés dans les bureaux principaux pour différentes raisons, comme le scan des votes de référence du bureau de vote ou l'annulation de bulletins de vote qui avaient été scannés mais pas encore déposés dans l'urne

4.3.1.3 Vérification et décryptage des clés USB

L'environnement de copie des supports mémoire du Collège a permis de procéder automatiquement à divers contrôles :

- comparaison des contenus des deux clés d'un même bureau ;
- comparaison des logiciels systèmes d'exploitation, logiciels exécutables et des jeux de données (communes, listes, candidats, etc.) avec ceux d'une clé USB de référence ;
- vérification et décryptage des fichiers « .VT » des clés.

Le Collège n'a constaté aucune anomalie dans les clés lisibles récupérées et est convaincu de leur authenticité. Les procédures en place, les sécurités cryptographiques en place lui permettent également de conclure qu'il s'agit bien des clés USB authentiques utilisées dans les différents bureaux de vote lors des élections.

Au moyen d'un outil logiciel reçu de SmartMatic (et dont le code source est disponible) et des différents mots de passe reçus du SPF Intérieur, le Collège a procédé au décryptage de tous les fichiers de type « .VT » en sa possession.

Le Collège a ainsi pu obtenir pour chaque bureau de vote (dont il avait au moins une clé) les fichiers « .VT » décryptés.

Étant donné les systèmes cryptographiques et de signature digitale en vigueur dans le système, ainsi que le décryptage sans erreur de tous les fichiers « .VT », le Collège est convaincu de l'authenticité des votes enregistrés sur les clés USB.

4.3.1.4 Copie des fichiers « .VT » pour les clés manquantes

Au moment de la lecture des clés USB dans le bureau de canton en vue de la collecte des résultats, le système Martine récupère également les fichiers « .VT » et les stocke sur un serveur central.

Pour pallier aux clés USB manquantes dans 3 cantons, le Collège a demandé et obtenu de Civadis, par l'intermédiaire du SPF Intérieur, une copie des fichiers « .VT » enregistrés par le système Martine le soir des élections.

Ces fichiers ont été décryptés au moyen des mots de passe correspondant au bureau de vote où ils ont été émis.

Étant donné les systèmes cryptographiques et de signature digitale en vigueur dans le système, ainsi que le décryptage sans erreur de ces fichiers « .VT », le Collège est convaincu de leur authenticité.

4.3.1.5 Retotalisation complète des clés USB par commune

Une fois les fichiers « .VT » décryptés, le Collège a utilisé un logiciel qu'il a développé pour effectuer une retotalisation complète de tous les fichiers « .VT » pour tous les bureaux de vote de toutes les communes.

4.3.1.6 Récupération des données transmises aux médias

En vue de capter les résultats publiés, le Collège s'est conformé à la procédure prévue pour les médias. Il s'agissait de mettre en place un serveur SFTP (serveur de fichiers sécurisé) sur lequel le SPF Intérieur met, via le système Martine, périodiquement les résultats intermédiaires et, dès que disponibles, les résultats finaux.

Cela a permis non seulement de saisir les résultats, mais aussi de suivre à quel moment les résultats ont été envoyés.

Les fichiers reçus ont été stockés dans une base de données locale au moyen d'un logiciel propre au Collège afin de les comparer avec les résultats obtenus après la retotalisation (voir ci-dessus).

4.3.1.7 Vérification de la retotalisation

Sur la base des totaux ainsi obtenus, le Collège a procédé à diverses vérifications tant sur les chiffres électoraux que sur les voix de préférence et les votes blancs tels que repris sur le site web officiel des élections. Il n'a découvert aucune discordance lors de ces contrôles.

De plus, pour toutes les élections, une comparaison automatisée et intégrale a été effectuée au niveau des résultats par commune, tant au niveau du chiffre électoral de chaque liste que des voix de préférence de chaque candidat et des votes en tête de liste.

Là non plus, le Collège n'a constaté aucune différence entre sa retotalisation et les données diffusées par le système Martine.

4.4 Diffusion du code source

4.4.1 Code source des logiciels SmartMatic

Le Collège a pu constater que le code source avait bien été publié sur le site du SPF Intérieur.

Le Collège a comparé ces sources avec celles reçues de SmartMatic lors de la compilation de référence pour produire les exécutables utilisés le jour des élections. Le code source publié est identique à celui obtenu de SmartMatic à l'occasion de la compilation de référence.

4.4.2 Code source du système Martine

La loi ne prévoit pas la publication du code source du système Martine.

5 Recommandations

5.1 Recommandations faisant suite au problème de transmission des résultats

[#2019-BE.1] Le Collège recommande de réviser le « disaster recovery plan » en tenant compte de manière systématique de l'impact de chaque service tiers (DNS, authentification via eID, etc.).

[#2019-BE.2] Le Collège recommande de mettre à jour les machines servant à l'envoi des données dans les bureaux principaux et d'en limiter au maximum les accès non nécessaires (p.ex. au moyen d'un firewall logiciel).

[#2019-BE.3] Le Collège recommande de mener divers tests automatisés sur l'infrastructure réelle (et non simulée) plusieurs semaines avant les élections. Ces tests devraient, entre autres, éprouver les limites de charge de l'infrastructure en conditions réelles et permettre de vérifier l'adéquation du « disaster recovery plan ».

[#2019-BE.4] Le Collège recommande de concevoir le processus comme si l'envoi des données se faisait systématiquement sur un réseau public non sécurisé.

[#2019-BE.5] Le Collège recommande d'étendre la mission de PwC de manière à inclure l'analyse des ordinateurs de transmission des bureaux de cantons.

5.2 Recommandations concernant les procédures

[#2019-BE.6] Le collège a constaté lors de ses contrôles dans les bureaux de vote que beaucoup de présidents de bureaux éprouvaient des difficultés au niveau de la procédure de fermeture du bureau (formulaires à remplir, enveloppes à utiliser, etc.) Le Collège recommande que les formations en tiennent compte et adressent ces problèmes.

[#2019-BE.7] Le Collège d'experts recommande la mise à jour du plan de gestion d'incidents avec entre autres des procédures claires encadrant les incidents qui interviendraient avant, pendant ou après le jour des élections.

[#2019-BE.8] Le Collège d'experts recommande que le contenu des clés USB soit systématiquement effacé après les élections.

[#2019-BE.9] Le Collège d'experts recommande que les procédures prévoient une identification claire, nominative et précise des personnes intervenant dans les bureaux de vote et dans les bureaux principaux lors des élections, en particulier des techniciens.

[#2019-BE.10] Le Collège d'experts recommande que la partie textuelle du bulletin de vote contienne aussi le numéro de la liste, ainsi que le nom du canton ou de la commune dans lequel le vote a été émis.

[#2019-BE.11] Le Collège d'experts recommande que les électeurs soient informés et invités à relire la version lisible et la version encodée des votes qu'ils ont exprimés avant numérisation et insertion de ceux-ci dans l'urne.

Rapport du Collège d'experts – élections de 2019

[#2019-BE.12] Le Collège d'experts recommande que les codes sources satisfassent aux exigences et critères de qualité de l'état de l'art en méthodologie de développement sécurisé de logiciels.

[#2019-BE.13] Le Collège d'experts recommande que le développement des logiciels du système de vote se fasse au moyen d'outils de développement standard, dans un code clair, lisible et pertinemment commenté et documenté. Toutes les procédures et spécifications permettant de produire les exécutable doivent être clairement décrites, être rendues disponibles et pouvoir être aisément reproduites. Tous les programmes, les bibliothèques, leurs versions et leurs paramètres d'exécution doivent être documentés avec précision. Il s'agit d'appliquer les bonnes pratiques de développement.

[#2019-BE.14] Au vu des manquements constatés concernant le respect des procédures, le Collège d'experts recommande qu'un contrôle systématique soit effectué pour s'assurer de l'application de toutes les procédures.

[#2019-BE.15] Le Collège recommande que ses recommandations soient systématiquement lues, tout particulièrement la [#2019-BE.15].

[#2019-BE.16] Le Collège d'experts recommande de ne plus utiliser les algorithmes MD5 ou SHA-1, mais bien de passer à SHA-2 (SHA-512) ou SHA-3.

[#2019-BE.17] Le Collège d'experts recommande le nettoyage du code du système SmartMatic de manière à éviter tout code inutilisé dans le cadre des élections en Belgique.

[#2019-BE.18] Le Collège d'experts recommande que le nombre d'essais pour entrer un mot de passe soit limité et qu'une politique claire soit mise sur pied et documentée par le SPF Intérieur quant à ce qui se passe quand le nombre limite d'essais est dépassé (attente d'un délai avant de pouvoir recommencer ou bannissement).

[#2019-BE.19] Le Collège d'experts insiste pour que les résultats exhaustifs des élections soient rendus disponibles sur le site officiel des élections dans un format de données « open-data » (JSON, CSV...) afin de faciliter les contrôles.

5.3 Recommandations faisant suite aux rapports du CCB

Après lecture des rapports du CCB, les recommandations suivantes sont émises par le Collège.

[#2019-BE.20] Le Collège d'experts recommande l'amélioration du plan de crise, tant au niveau de l'infrastructure matérielle que logicielle et de le compléter par un plan de communication et/ou un « disaster recovery plan ».

[#2019-BE.21] Le Collège d'experts recommande que Martine soit développée de manière sécurisée, sans attendre que le CCB ne mène ses exercices en fin de cycle de développement.

[#2019-BE.22] Le Collège d'experts recommande de ne plus utiliser le chiffrement AES en mode CBC pour l'authentification.

Rapport du Collège d'experts – élections de 2019

[#2019-BE.23] Le Collège d'experts recommande que la documentation des systèmes soit générée et maintenue à jour pendant tout le cycle de développement et non uniquement à la fin.

[#2019-BE.24] Le Collège d'experts recommande de séparer les canaux de livraison des clefs USB et des mots de passe.

[#2019-BE.25] Le Collège d'experts recommande la mise en place d'un processus de génération des clés cryptographiques qui ne soit pas sensible au « key escrow problem » (extorsion de clés par celui qui la génère).

[#2019-BE.26] Le Collège d'experts recommande de mieux évaluer l'impact, en termes de sécurité, des interdépendances logicielles (bibliothèques externes ou open source) et des appels à des parties tierces (p.ex. pour l'authentification ou la DNS).

[#2019-BE.27] Le Collège d'experts recommande de mettre en place un système de sondes (IDS) qui permette de détecter tout trafic non désiré sur le réseau (autre que celui strictement nécessaire aux élections) et mettre en place une procédure pour nettoyer tout trafic indésirable.

[#2019-BE.28] Le Collège d'experts recommande que les systèmes utilisés dans les bureaux de canton pour la transmission de résultats soient composés d'un système d'exploitation et de logiciels libres, sécurisés et « **hardened** », à l'image de ce qui se fait pour les systèmes utilisés dans les bureaux de vote.

5.4 Recommandations générales

[#2019-BE.29] Le Collège d'experts recommande que l'interface des machines à voter soit évaluée par des experts en ergonomie vis-à-vis de l'état de l'art de la discipline.

[#2019-BE.30] Le Collège d'experts recommande que chaque fichier rendu public par le pouvoir organisateur concernant les élections (résultats, code source, etc.) soit publié avec hash et signature électronique correspondante. Le Collège d'experts recommande que ces documents soient disponibles de manière permanente sur un site avec fonction de recherche.

[#2019-BE.31] Le Collège demande que la législation concernant le vote électronique soit modifiée pour que les supports mémoires (clés "USB") utilisées le jour des élections soient transmises au plus tard le lendemain des élections à 15h au Collège d'experts.

[#2019-BE.32] Le Collège insiste pour que tous les éléments de configuration et de programmation soient présents dans le code source fourni par SmartMatic lors de la compilation de référence.

6 Conclusion

Suite à la modification de la législation, le Collège est maintenant compétent pour contrôler les systèmes de vote électronique mais également « *tout logiciel utilisé dans le cadre des élections même lorsque le vote se déroule selon d'autres modalités que celles prévues par la présente loi* ». La mission du Collège est donc étendue au système informatique utilisé dans les communes et cantons utilisant le vote traditionnel « papier ».

Comme précédemment, le Collège a surtout orienté ses travaux sur les éléments que lui seul pouvait légalement contrôler, en particulier la retotalisation des supports mémoires utilisés dans les bureaux de votes électroniques. Il n'a donc pas procédé à un contrôle exhaustif des résultats de comptage et de totalisation pour le vote traditionnel, le contrôle démocratique dans les bureaux de dépouillement et dans les bureaux de cantons concernés étant assuré par les dispositions légales en vigueur.

Dans les limites de la mission, des moyens et du temps disponibles, le Collège conclut ce qui suit :

- pour les communes et cantons faisant usage du vote électronique, le Collège n'a détecté aucune différence entre les résultats communiqués aux médias par le système Martine et publiés sur le site officiel des élections et la retotalisation exhaustive qu'il a faite à partir des clés USB. Le Collège en conclut par conséquent que les systèmes ont correctement récolté et totalisé les voix pour ces cantons et communes ;
- pour les communes faisant usage du vote traditionnel, le Collège n'a pas eu vent de problèmes, d'erreurs ou d'incohérences dans les résultats encodés à partir des PVs des bureaux de dépouillement et des PVs des bureaux de canton. Il considère que de tels problèmes, erreurs ou incohérences peuvent être détectés par ces bureaux eux-mêmes.

Le Collège estime donc que le problème de transmission des résultats survenu le soir des élections n'a pas eu d'impact sur les résultats de celles-ci.

Par conséquent, le Collège estime que l'objectif d'émettre les votes, de les enregistrer et de les compter selon les dispositions légales, a été atteint.

Le Collège remercie tous les intervenants avec qui il a travaillé pendant sa mission de contrôle pour leur coopération : les représentants des firmes, de l'organisme d'avis et du CCB, les membres des bureaux de vote et des bureaux principaux ainsi que le personnel des communes.

Il tient tout particulièrement à remercier les représentants du SPF Intérieur pour leur excellente collaboration, leur disponibilité et leur réelle volonté de transparence en particulier lors de l'analyse du problème de transmission des résultats.

Rapport du Collège d'experts – élections de 2019

Bruxelles, le 7 juin 2019.

Pour le Collège

Emmanuel Willems
Président

Bart Martens
Secrétaire

**Verslag van het College van Deskundigen belast met
de controle van het elektronisch stem- en
stemopnemingsysteem**

**Gelijktijdige verkiezingen van 26 mei 2019 voor het
Europees Parlement, de Kamer van
Volksvertegenwoordigers en de Gemeenschaps- en
Gewestparlementen**

Brussel, 7 juni 2019

Inhoudstafel

1	Het College	4
1.1	Samenstelling van het College	4
1.2	Het niet-permanent College	4
1.3	De opdracht	5
1.4	Het verslag.....	6
1.5	Geheimhouding	6
1.6	Ter beschikking stellen van de nodige middelen	6
2	De wetgeving	7
2.1	Wijzigingen met betrekking tot de stelsystemen	7
2.2	Wijzigingen betreffende de publicatie van de broncodes.....	7
2.3	Wijzigingen betreffende het College van Deskundigen	7
3	Beschrijving van de systemen	8
3.1	Globale functionele beschrijving.....	8
3.2	SmartMatic	8
3.2.1	Functionele beschrijving	8
3.2.2	Stemprocedure met papieren bewijsstuk	9
3.2.3	Technische elementen van het in de stembureaus gebruikte systeem SmartMatic	10
3.3	Martine	11
3.3.1	Infrastructuur.....	11
3.3.2	Software.....	12
4	Controles en vaststellingen	14
4.1	Controles vóór de dag van de verkiezingen	14
4.1.1	Controles van het SmartMatic systeem	14
4.1.2	Controles van het systeem Martine – module MA2X.....	18
4.1.3	Relaties tussen de bedrijven verantwoordelijk voor de ontwikkelingen	19
4.1.4	Analyse van de broncode	19
4.1.5	Analyse door het CCB.....	20
4.1.6	Bezoek aan het datacenter van FOD BiZa	21
4.1.7	Deelname aan de opleidingen.....	21
4.1.8	Naleving van de procedures.....	22
4.2	Vaststellingen op de verkiezingsdag.....	23
4.2.1	Controles in de stembureaus	23
4.2.2	Incidenten in de stembureaus.....	25
4.2.3	Controles in de hoofdbureaus.....	27
4.2.4	Incident : Voortijdige publicatie van resultaten op de websites van de media.....	27
4.2.5	Incidenten met het doorsturen van de resultaten door de kantons op de avond van de verkiezingen.....	28
4.3	Na de verkiezingsdag uitgevoerde controles	30
4.3.1	Verificatie van de totalisaties	30
4.4	Verspreiding van de broncode	32
4.4.1	Broncode van de SmartMatic-software	32
4.4.2	Broncode van het systeem Martine	32
5	Aanbevelingen	33

Verkiezingen 2019 - Verslag van het College van Deskundigen

5.1	Aanbevelingen ten gevolge van het probleem met het doorsturen van de resultaten	33
5.2	Aanbevelingen betreffende de procedures	33
5.3	Aanbevelingen naar aanleiding van de verslagen van de CCB.....	34
5.4	Algemene aanbevelingen	35
6	Besluit.....	37

1 Het College

1.1 Samenstelling van het College

Op grond van artikel 24 van de wet van 7 februari 2014 zoals gewijzigd door de wet van 19 april 2018 tot organisatie van de elektronische stemming met papieren bewijsstuk, zijn de Deskundigen, waarvan de namen volgen, aangewezen voor een duurtijd van vijf jaar om het permanent College te vormen:

Deskundigen aangewezen door de Kamer van Volksvertegenwoordigers:

- effectief: de heer Bruno DE NYS, de heer Karel VAN GEYT en de heer Jérôme DOSSOGNE;
- plaatsvervangend: Mevrouw Sophie JONCKHEERE, de heer Jean-Marc Paul en de heer Erwin VEREECKEN.

Deskundigen aangewezen door het Vlaams Parlement:

- effectief: de heer Bart MARTENS;
- plaatsvervangend: de heer Romain VOES.

Deskundigen aangewezen door het Brussels Hoofdstedelijk Parlement:

- effectief: de heer Emmanuel WILLEMS;
- plaatsvervangend: de heer Pascal VAN de WALLE.

Deskundigen aangewezen door het Parlement van de Duitstalige Gemeenschap:

- effectief: de heer Daniel BRANDT;
- plaatsvervangend: Mevrouw Susi SARLETTE OSTLENDER.

Deze experts vormen het permanent College van Deskundigen.

Het Waals Parlement heeft geen deskundigen aangewezen voor dit permanent College.

Overeenkomstig artikel 24 §2 derde lid van de wet van 7 februari 2014 wijzen de effectieve deskundigen in hun midden een voorzitter, de heer Emmanuel WILLEMS, en een secretaris, de heer Bart MARTENS aan.

1.2 Het niet-permanent College

In overeenstemming met artikel 24, § 3 van de wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstuk, zijn de deskundigen, waarvan de namen volgen, aangewezen om het niet-permanent College te vormen ter gelegenheid van de gelijktijdige verkiezingen van 26 mei 2019 voor het Europees Parlement, de Kamer van volksvertegenwoordigers en de Gewest- en Gemeenschapsparlementen:

Deskundigen aangewezen door de Kamer van Volksvertegenwoordigers: de heer Bruno PENNE en de heer Pol BADOUX.

Verkiezingen 2019 - Verslag van het College van Deskundigen

Deskundigen aangewezen door het Waals Parlement: de heer Jean-François DAMSEAUX en de heer Alexandre DUBOIS.

Deskundigen aangewezen door het Vlaams Parlement: de heer Romeo MARYNS en de heer Steven ES.

Deskundigen aangewezen door het Brussels Hoofdstedelijk Parlement: de heer Fabrice DUMORTIER en de heer Jean-Michel DRICOT.

Deskundigen aangewezen door het Parlement van de Duitstalige Gemeenschap: de heer Bruno HICK en de heer Andreas SCHENK.

1.3 De opdracht

De rol, missie en middelen van het College zijn vastgelegd in de wet van 7.02.2014, hoofdstuk 7, art.25 zoals gewijzigd door de wet van 19 april 2018, waarvan de tekst als volgt luidt:

“§ 1. Bij de verkiezing van de leden van de Kamer van volksvertegenwoordigers, van het Europees Parlement en de Gewest- en Gemeenschapsparlementen, zien deze deskundigen toe op de voorbereiding, het gebruik en de goede werking van alle elektronische stemsystemen, registratiesystemen, ontsleutelingssystemen en totaliseringssystemen, alsook de procedures betreffende de aanmaak, de verspreiding en het gebruik van de apparatuur, programmatuur en de elektronische gegevensdragers. Het College van Deskundigen controleert eveneens de voorbereiding, het gebruik en de goede werking van de hardware, software en procedures voor de digitale transmissie en het digitaal verspreiden van de resultaten alsook alle software die gebruikt wordt in het kader van de verkiezingen, zelfs als er op traditionele wijze gestemd wordt.

De deskundigen ontvangen van de minister van Binnenlandse Zaken of zijn afgevaardigde het materiaal alsook alle gegevens, inlichtingen en informatie die nuttig zijn om een controle uit te voeren op de elektronische stemsystemen, de registratiesystemen en de totaliseringssystemen en op de systemen van digitale doorzending van de resultaten. De leden van de kiesbureaus, de in artikel 4, § 3, tweede lid, bedoelde adviesorganen en de privébedrijven — alsook hun leden — die door de bevoegde overheden betrokken zijn bij het verloop van het kiesproces leveren eveneens aan de deskundigen het materiaal alsook alle gegevens, inlichtingen en informatie die nodig zijn om de in het eerste lid bedoelde controle uit te voeren.

De deskundigen kunnen in het bijzonder — tijdens de verkiezing — stemmen uitbrengen die gescand noch geteld worden, de betrouwbaarheid controleren van de software in de stemsystemen, alsook de correcte overschrijving van de uitgebrachte stemmen op de stembiljetten, de correcte overschrijving, door het lezen van de barcode op elk stembiljet, van de uitgebrachte stemmen op de gegevensdrager van het stembureau, de correcte registratie van de gegevensdrager van het stembureau op de gegevensdrager bedoeld voor het optellen van de stemmen en de totalisering van de uitgebrachte stemmen. Ze kunnen eveneens de betrouwbaarheid nagaan van de software voor het digitaal doorsturen van de verkiezingsuitslagen.

Verkiezingen 2019 - Verslag van het College van Deskundigen

Het College van Deskundigen kan overgaan tot een audit van de uitslagen om de betrouwbaarheid en integriteit van het elektronische stelsysteem met afdruk van een papieren stembiljet te verzekeren.

Zij verrichten de controle vanaf de veertigste dag voor de verkiezing, op de verkiezingsdag zelf en hierna tot de indiening van het in § 2 bedoelde verslag.”

1.4 Het verslag

“§ 2. Uiterlijk vijftien dagen na de sluiting van de stemming en in ieder geval voor de geldigverklaring van de verkiezingen voor wat de Kamer van Volksvertegenwoordigers, de Gewest- en Gemeenschapsparlamenten en het Europees Parlement betreft, bezorgen de deskundigen een verslag aan de minister van Binnenlandse Zaken, alsook aan de federale wetgevende assemblees en de Gewest- en Gemeenschapsparlamenten.”

1.5 Geheimhouding

“§ 3. De deskundigen zijn tot geheimhouding verplicht. Elke schending van de geheimhoudingsplicht wordt bestraft overeenkomstig artikel 458 van het Strafwetboek.”

1.6 Ter beschikking stellen van de nodige middelen

“§ 4. De Kamer van Volksvertegenwoordigers zorgt ervoor dat de nodige middelen voor de uitvoering van de in dit artikel bedoelde taken ter beschikking gesteld worden van het College van Deskundigen.”

2 De wetgeving

Sinds de laatste gelijktijdige verkiezingen in 2014 heeft de wetgeving inzake elektronische stemsystemen enige wijzigingen ondergaan die hieronder hernoemen worden.

2.1 Wijzigingen met betrekking tot de stemsystemen

Twee aanpassingen werden aan de stemsystemen aangebracht:

- een systeem van automatische afsluiting van de gleuf van de urne is toegevoegd om te voorkomen dat de kiezer zijn stembiljet in de urne plaatst voordat hij het heeft gescand. De gleuf wordt automatisch geopend nadat het bulletin is gescand en blijft enkele seconden open. Het sluit dan om te wachten op het volgende stembiljet;
- om het stemmen van visueel gehandicapte of blinde kiezers te vergemakkelijken, werd één van de stemcomputers in de stembureaus in Aalst en Mechelen voorzien van een elektronische doos waarmee een blinde of slechtziende kiezer zijn stem autonoom kan uitbrengen en dit zonder het touchscreen te gebruiken.

2.2 Wijzigingen betreffende de publicatie van de broncodes

De broncodes worden gepubliceerd door FOD BIZA in de week na de verkiezingen. Ze bevatten geen veiligheidselementen en blijven toegankelijk voor een periode van 6 maanden.

2.3 Wijzigingen betreffende het College van Deskundigen

- de leden van het permanent College worden benoemd 3 maanden vóór de verkiezing van het Europees Parlement. Ze blijven benoemd tot een nieuwe aanwijzing plaatsvindt;
- de rol van het College van Deskundigen wordt uitgebreid tot alle software die bij verkiezingen wordt gebruikt, zelfs wanneer er niet elektronisch wordt gestemd;
- de Kamer van volksvertegenwoordigers zal het Permanente College van Deskundigen de middelen ter beschikking stellen die nodig zijn voor het vervullen van haar taken;
- de Kamer van volksvertegenwoordigers of een Gemeenschaps- of Gewestparlement kunnen het permanent College van Deskundigen belasten met specifieke controle- en studieopdrachten met betrekking tot de beveiliging en betrouwbaarheid van de verschillende bij de verkiezingen gebruikte systemen, software en hardware.

3 Beschrijving van de systemen

Twee systemen moeten worden bekeken met betrekking tot de controle van het College:

1. het "Martine" -systeem, ontwikkeld door het bedrijf Civadis, dat verantwoordelijk is voor het verzamelen van basisgegevens (lijsten, kandidaten, betrokkenen, enz.) voor de verkiezing, het verzamelen van resultaten van stembureaus of telkantoren; berekening en verspreiding van verkiezingsresultaten;
2. het elektronische stemsysteem ontwikkeld door het bedrijf SmartMatic en gebruikt in 157 gemeenten van het Vlaamse Gewest, de 19 gemeenten van het Brussels Hoofdstedelijk Gewest en 9 gemeenten van de Duitstalige gemeenschap

Deze systemen zijn in wezen identiek aan die gebruikt in de gemeenteraadsverkiezingen van 2018.

3.1 Globale functionele beschrijving

Vóór de verkiezingen, dient het systeem Martine onder meer om de gegevens van de kandidaten te verzamelen om de lijsten op te stellen. De informaticabestanden die daarbij worden aangemaakt, worden geïntegreerd in de omgeving van SmartMatic, die dient om de USB-sticks aan te maken die op de dag van de verkiezingen worden gebruikt.

Op de dag van de verkiezingen, bij het afsluiten van de verrichtingen in het stembureau, maakt de machine van de voorzitter een "X7S"-resultaatbestand per verkiezing aan dat de in zijn stembureau uitgebrachte stemmen totaliseert.

In het hoofdbureau brengt het systeem Martine het resultaatsbestand over naar een centrale server die de totalisatie van alle stembureaus van de gemeente uitvoert, de volledige uitslag van de verkiezing berekent en verspreidt.

In de kantons waar nog op papier gestemd wordt het systeem Martine gebruikt om de resultaten van de telbureaus in te geven.

3.2 SmartMatic

3.2.1 Functionele beschrijving

Het SmartMatic-systeem is beschikbaar in twee versies: de versie die voor het eerst werd gebruikt in 2012 en een versie die in 2018 werd gebruikt in de gemeenten die voor de verkiezingen van 2018 of 2019 besloten hebben om over te stappen op het elektronisch stemmen.

3.2.1.1 De urne en de machine van de voorzitter

De versie 2012 bestaat uit een draagbare computer waarop een USB-hub met twee dezelfde USB-sticks is aangesloten, een elektronische urne en een lezer-opnemer van chipkaarten. De USB-sticks bevatten alle software van het stembureau, zowel voor de machine van de voorzitter als voor de stemmachines. De urne omvat een

Verkiezingen 2019 - Verslag van het College van Deskundigen

reservoir dat de door de stemmachines afgedrukte stemmen opvangt. Daar bovenop staat een scanner voor de QR-codes.

Bij de versie 2018, bestaat de pc van de voorzitter van het stembureau uit een pc met geïntegreerd touchscreen, die verbonden is met de USB-hub van de urne, die tevens voor de voeding zorgt.

3.2.1.2 De stemmachine

De stemmachine SmartMatic is een computer met standaardcomponenten die in een specifieke behuizing is geplaatst met een touchscreen, een chipkaartlezer en een geïntegreerde printer. De schakelaar, de stekker voor de aansluiting op het stroomnet, de USB-poorten en de aansluiting van het alarm bevinden zich aan de achterzijde. De enige componenten van de computer waartoe de kiezer toegang heeft, zijn de chipkaartlezer en de printer die zich aan de voorzijde bevinden. Een stemmachine heeft geen toetsenbord noch een harde schijf.

In twee kantons (Aalst en Mechelen) die experimenteren met een audio-interface voor slechtzienden en blinden, bevatten de stemmachines een doos die toelaat om een audiokoptelefoon aan te sluiten en die beschikken over toetsen voor de navigatie en de selecties van de verkiezingen, de lijsten en de kandidaten.

Bij de verkiezing werden twee versies van de stemmachine gebruikt: de originele versie van 2012 en een nieuwe versie van 2018. De twee versies verschillen door de omvang van het apparaat en de positie van de chipkaartlezer en de printer. Voor het overige bieden ze precies dezelfde functionaliteiten aan.

3.2.2 Stemprocedure met papieren bewijsstuk

3.2.2.1 Opening van het stembureau met papieren bewijsstuk

De eerste verrichting bestaat erin de machine van de voorzitter op te starten met de twee identieke USB-sticks die hij tegelijk met zijn wachtwoorden krijgt.

De voorzitter en zijn bureau controleren of de verschillende componenten goed aangesloten zijn en starten de machine van de voorzitter op. Vervolgens wordt een diagnose gesteld van de machine van de voorzitter en de aangesloten randapparatuur (USB-sticks, urne, kaartlezer, toetsenbord, muis...).

De machine van de voorzitter vraagt om de stemmachines op te starten. Daartoe heeft men één van de USB-sticks nodig. Wanneer alle stemmachines opgestart zijn, worden de USB-sticks opnieuw aangesloten op de machine van de voorzitter.

3.2.2.2 Het verloop van de stemming

De stemming gebeurt op de stemmachine in het stemhokje. De stemmachine drukt een papieren bewijsstuk af met daarop de stemmingen in leesbare vorm en in de vorm van een QR-code.

Elke kiezer krijgt een geïntialiseerde chipkaart waarmee hij kan stemmen. Hij neemt die kaart mee in het stemhokje en steekt ze in de stemmachine. Een kaart die slecht of niet geïntialiseerd werd of al gebruikt werd, wordt geweigerd. De kaart

Verkiezingen 2019 - Verslag van het College van Deskundigen

dient enkel om de stemverrichting te starten en bevat geen andere informatie. Ze dient niet om de stem op te slaan.

Op het scherm verschijnen aanwijzingen tijdens de hele kiesverrichting. De kiezer wordt verzocht de taal van de interface te kiezen. Vervolgens kan hij zijn stem (blanco stem, lijststem, voorkeurstemmen) uitbrengen voor elke verkiezing die het systeem hem voorstelt. In elke fase, wordt hij verzocht zijn keuze te bevestigen alvorens naar de volgende fase over te gaan. Wanneer de kiezer zijn stem heeft bevestigd door op het touchscreen een bepaalde verkiezing, is de stemming definitief; de kiezer kan zijn stem niet meer veranderen. Zolang de kiezer zijn stem niet heeft bevestigd, kan hij zijn stem annuleren en herbeginnen.

Na bevestiging van de stem, drukt de stemmachine de stem af in de vorm van tekst en in de vorm van een QR-code op een “papieren bewijsstuk” en vraagt de kiezer om de chipkaart terug te nemen. In een daartoe bestemd stemhokje, kan de kiezer de QR-code van zijn papieren bewijsstuk scannen met een draagbare scanner. De inhoud van de QR-code wordt dan getoond op het scherm en de kiezer kan zijn stem controleren.

Vervolgens begeeft de kiezer zich naar de urne, waar hij verzocht wordt de QR-code van zijn stembiljet boven de scanner van de urne te houden. Na een auditieve en visuele bevestiging dat de QR-code wel degelijk gelezen en geregistreerd is door de computer van de voorzitter, steekt de kiezer zijn bewijs op papier in de urne en overhandigt hij de chipkaart aan de voorzitter of een bijzitter.

3.2.2.3 Sluiting van het stembureau

Na afloop van de stemming, wordt het stembureau gesloten en wordt een verslag met de USB-sticks gedrukt. Het verslag wordt met de hand ondertekend door de leden van het stembureau en bij hun proces-verbaal gevoegd.

De urne wordt geopend en de bulletins “papieren bewijstukken” worden in een envelop gestoken. De envelop met de stembiljetten wordt vervolgens verzegeld. Het proces-verbaal, de usb-sticks van het stembureau en de verzegelde envelop met de stembiljetten worden meegenomen naar het hoofdbureau.

3.2.3 Technische elementen van het in de stembureaus gebruikte systeem SmartMatic

Het in de stembureaus gebruikte systeem SmartMatic wordt uitgevoerd vanaf de geheugendragers van het type USB-stick. De USB-sticks bevatten alle programma's en alle gegevens die nodig zijn voor de werking van de verschillende computers (machine van de voorzitter en stemmachine) en randapparatuur (urne en handscanner in het stemhokje).

De USB-sticks worden centraal aangemaakt en zijn volledig identiek voor alle stembureaus, zowel bij de versie 2012 als de versie 2018 van de apparatuur SmartMatic. Ze worden pas specifiek voor een stembureau na de eerste opstart en de invoering van de naam van het stembureau en het overeenkomstige wachtwoord.

Verkiezingen 2019 - Verslag van het College van Deskundigen

Vanaf dat moment kunnen de USB-sticks enkel nog voor dat specifieke stembureau worden gebruikt.

Voorts bevat de USB-stick twee opslagzones, in het computerjargon “partities” genoemd: de ene is specifiek voor de programma’s die in het stembureau draaien op de dag van de verkiezingen. In dit verslag wordt deze partitie de “partitie SmartMatic” genoemd. De andere partitie dient voor het opslaan van de gegevens en de uitslag van het stembureau, die moeten worden overgebracht naar de omgeving Martine voor de totalisatie per gemeente en de berekening van de uitslag per gemeente. In dit verslag, wordt die partitie de “partitie Martine” genoemd.

3.2.3.1 Partitie SmartMatic

Voor elk door de urne gescand stembiljet, wordt een kopie van de uitgebrachte stem opgeslagen in een bestand met extensie “.VT” in de map “/SAESLocal/SAES/Votes” van de USB-stick. Op het einde van de dag, bevat die map evenveel bestanden “.VT” als gescande stembiljetten.

Wanneer de stemverrichtingen worden afgesloten, wordt per verkiezing een resultatenbestand met extensie “.X7S” aangemaakt. Die bestanden worden digitaal ondertekend en zo versleuteld dat ze enkel gedecodeerd kunnen worden door de applicatie Martine, die ze moet totaliseren.

3.2.3.2 Partitie Martine

Bij het sluiten van het stembureau, worden de “.VT”- en “.X7S”-bestanden en enkele andere controlebestanden vanuit de partitie SmartMatic gekopieerd naar de partitie Martine.

Onder de controlebestanden, bevindt zich het pdf-bestand dat dient om het “kerncijferrapport” af te drukken in het stembureau.

3.3 Martine

Martine is een multitask online platform dat onder meer voor het volgende zorgt : het beheer van de structuur van de verkiezing, de naam en het aantal hoofdbureaus, het aantal stembureaus per gemeente en het adres ervan, de contacten, de akten van indiening, de processen-verbaal van stopzetting, de processen-verbaal van stemopneming, de uitslag van de stemming.

De bij Martine betrokken actoren zijn:

- de gemeenten;
- de hoofdbureaus;
- de kandidaten;
- de organiserende overheid.

3.3.1 Infrastructuur

De oplossing is gebaseerd op een gevirtualiseerde omgeving op basis van een distributie Linux Centos/Redhat en VMware ESXi hypervisor. De applicatie wordt over minimum 3 servers verdeeld. Alle modules worden op redundante wijze

Verkiezingen 2019 - Verslag van het College van Deskundigen

ontplooid volgens het principe van de werkwijze “actief/actief”. De databases en het filesysteem server werken in de modus “actief/passief”.

Minstens twee redundante lijnen zijn beschikbaar, de ene in productie en de andere in alarm. De hoofddatabase en de back-updatabase worden continu gesynchroniseerd. De infrastructuur is uitgerust met redundante elektrische voeding, internetverbindingen, switches, firewalls,...

3.3.2 Software

Martine wordt opgebouwd uit een geheel van softwarecomponenten die in drie categorieën kunnen worden ingedeeld :

- “Web modules”, ontworpen voor de gebruikers ;
- “Back end modules”, om de gegevens en resultaten van de kandidaten op de achtergrond te beheren ;
- “Ondersteuning modules” voor intern gebruik voor specifieke taken.

3.3.2.1 De modules

Martine bestaat uit de volgende modules:

3.3.2.1.1 MA1X (Web)

MA1X biedt tools aan voor de voorbereiding van de kieslijsten.

3.3.2.1.2 MA2X (Web)

MA2X wordt gebruikt door het team van het hoofdbureau om de stemmen te verzamelen. Voor de stembureaus “op papier”, wordt de data manueel ingevoerd in het systeem. In de elektronische stembureaus worden de stemgegevens verkregen door het inpluggen van de USB-stick SmartMatic. De gelezen bestanden (“.X7S” en “.VT”) worden overgebracht naar MA2X en geregistreerd voor latere verwerkingen.

MA2X zorgt ook voor de productie van partiële en definitieve resultaten door het hoofdbureau.

3.3.2.1.3 MA3X (Web)

MA3X bevat de informatie over de stembureaus en de telbureaus: adressen en contactpersonen, de voorzitter en de secretaris van het bureau enzovoort.

MA3X wordt ook gebruikt door MA1B (zie hierna) en MA2X om de toegang toe te staan aan gemachtigde gebruikers.

3.3.2.1.4 MA1L

MA1L dient voor de voorbereiding van de akten van indiening van de kandidaten.

3.3.2.1.5 MA1B (Web)

MA1B ontvangt de akten van de kandidaatstellingen voordat een definitief proces-verbaal opgemaakt wordt met de gedetailleerde lijsten van MA1X. MA1B registreert ook de afgewerkte lijsten in backend Martine.

3.3.2.1.6 MA3S

MA3S superviseert de operaties die de gemeenten en de hoofdbureaus in MA3X uitgevoerd hebben. De modules “Collect” en “Calc” maken het mogelijk de aankomst van de bestanden op de centrale servers van de organiserende overheid te volgen. De module “Cockpit” maakt het mogelijk alle operaties van alle modules op te volgen.

3.3.2.1.7 DECRYPT (Ondersteuning)

DECRYPT is een dienstinterface voor MA2X zodat het die informatie kan lezen en doorsturen vanuit bestanden met gecijferde stemresultaten. Het is een aparte module, enkel voor de veiligheid. De interface is niet toegankelijk vanop het internet en kan dus meer gescheiden worden van het netwerk om de controle op de toegang te optimaliseren. De ontcijfering vereist de private ontcijferingssleutel voor de bestanden die op USB-sticks gelezen worden.

3.3.2.1.8 MA1-COLLECT (Backend)

MA1-COLLECT is het voornaamste ingangspunt met toezichtsinterface voor de bestanden die aangemaakt worden. Het voert een eenvoudige validering van de ontvangen bestanden uit en slaat die op voor latere verwerking door MA2-CALCULATE. MA1-COLLECT wordt ook gebruikt door MA2X om de gegevens van de resultaten te lezen die nodig zijn voor de productie van de uiteindelijke PV's.

3.3.2.2 Toegang tot de modules

De toegang tot de modules voor de gemeenten, de hoofdbureaus en de politieke partijen is afhankelijk van de invoering van een elektronische identiteitskaart met bijhorende pincode. Die modules zijn de volgende : MA3X, MA1L, MA1B, MA2X.

De gebruikers van de modules MA3X zijn vóór de verkiezing niet gekend door de inrichtende overheid. Die worden intern aangesteld door de gemeenten (MA3C) of door de voorzitters van de hoofdbureaus (MA3B). Een SPOC-systeem (single point of contact) is uitgewerkt om een bureau te laten samenwerken met zijn gebruikers. Martine koppelt aan elk hoofdbureau een login/wachtwoord dat overgezonden wordt aan de bureaus in kwestie via de officiële weg uitgestippeld door de inrichtende overheid.

Wie over het login/wachtwoord van het bureau beschikt, kan inloggen in MA3X met zijn identiteitskaart en pincode. Die persoon wordt dan de voornaamste SPOC voor dat bureau en kan later toegang tot de module krijgen door enkel zijn identiteitskaart te gebruiken. Het gebruik van login/wachtwoord is enkel nodig voor de eerste verbinding.

Een SPOC kan een backup-SPOC aanstellen in zijn bureau.

4 Controles en vaststellingen

4.1 Controles vóór de dag van de verkiezingen

4.1.1 Controles van het SmartMatic systeem

4.1.1.1 Overhandiging van de source code en referentiecompilatie

Een vergadering voor het overhandigen van de broncode en een referentiecompilatie werd georganiseerd op 27 februari 2019 in de FOD BiZa in het bijzijn van het adviesorgaan, vertegenwoordigers van de firma SmartMatic en leden van het College van Deskundigen.

De oorspronkelijk geplande vergadering moest een week worden uitgesteld. Er was inderdaad een incompatibiliteit tussen de SmartMatic- en Martine-systemen ontdekt op het niveau van de berekeningsmodi van bepaalde beveiligingselementen.

Tijdens deze bijeenkomst presenteerde SmartMatic de wijzigingen die werden aangebracht aan de elektronische stemsystemen, die voornamelijk voortvloeien uit aanbevelingen van de Colleges van Deskundigen (federaal of regionaal) of uit het Centre for Cyber Security Belgium (CCB), waaronder:

- Activering van chipkaarten
- Aanwezigheid van een klep van de urne
- Update van cryptografische algoritmen
- Update van algoritmen voor digitale vingerafdrukken (hash-code)
- Geautomatiseerde generatie van initialisatiecodes
- Lijsten met typografische tekens die in wachtwoorden kunnen worden gebruikt
- Methode voor het invoeren van het wachtwoord
- Groter lettertype voor de partijnamen afgedrukt op de stembiljetten
- Beheer van de voortijdige extractie van USB-sticks (na het incident van 2018)
- Audiomodule voor navigatie en selectie van lijsten en kandidaten voor visueel gehandicapte kiezers
- Het verslag van het stembureau afdrukken door een stemmachine in plaats van een inkjetprinter
- FAT32-partitie voor de overdracht van de resultaten van het stembureau

Sommige waren al geïmplementeerd tijdens de verkiezingen van 2018.

De applicatie werd vervolgens gecompileerd op een lege pc. De gevolgde procedure verliep als volgt:

- Opstarten van de compilatie-pc op een USB-stick met een Linux Ubuntu 14.04 LTS-besturingssysteem
- Installeren van Ubuntu 14.04 LTS op de compilatie-pc
- Herstarten van de compilatie-pc onder Ubuntu en kopie van de broncode geleverd door SmartMatic

Verkiezingen 2019 - Verslag van het College van Deskundigen

- Compilatie en generatie van de disk image van de ECM-omgeving (voorbereidingsmachine)
- Compileren en genereren van de disk image van de voorzittersmachine (PM) en de stemmachine (VM)

Op het einde van de compilatie werden een kopie van de broncode en gegenereerde disk images op verschillende USB-sleutels gekopieerd. Deze USB-sleutels werden in verzegelde enveloppen afgegeven aan het adviesorgaan, het College en vertegenwoordigers van de firma SmartMatic.

Een kopie werd tevens in een verzegelde envelop geplaatst om in een kluis te worden gelegd en een laatste kopie, in een verzegelde envelop, werd afgegeven aan de FOD BiZa voor de volgende stappen die leidden tot het aanmaken van USB-sleutels voor gebruik op de verkiezingsdag.

Ten slotte gingen vertegenwoordigers van de FOD BiZa, het College, het adviesorgaan en SmartMatic naar het bankfiliaal voor het plaatsen in de kluis.

4.1.1.2 Verslag van het adviesorgaan

Het goedgekeurde adviesorgaan voor elektronische stemsystemen zoals beschreven in artikel 4, § 3 van de wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstukken voor de verkiezingen voor het Europees Parlement, de Kamer en de Gemeenschaps- en Gewestparlementen in de gemeenten waar gebruik wordt gemaakt van een elektronisch stelsysteem met papieren bewijsstuk is PricewaterhouseCoopers (PwC).

Het bedrijf PwC heeft een mandaat gekregen voor het nagaan van de geschiktheid van de applicaties van het systeem SmartMatic (overeenkomst PwC-SmartMatic van 23 januari 2019).

Tijdens een vergadering op 21 maart 2019 presenteerde het adviesorgaan PwC een voorverslag van zijn analyse van het SmartMatic-stelsysteem. Deze gefaseerde aanpak was essentieel om de compatibiliteit tussen SmartMatic en Martine in termen van gegevensuitwisseling te kunnen testen, omdat alle modules van Martine nog niet afgewerkt waren.

De analyse was gericht op de applicatie voor de voorbereiding van het stelsysteem met inbegrip van de duplicatie, het systeem van de bureauvoorzitter, de urne, de stemmachines en de applicatie voor de hertelling. PwC heeft heel wat geautomatiseerde controles uitgevoerd en heeft gesprekken gevoerd met het team belast met de ontwikkeling.

Het definitief advies werd op 12 april 2019 overhandigd.

De deskundigen hebben een kopie van het definitief advies van het adviesorgaan op 14 april 2019 ontvangen.

In dit advies wordt een hele reeks problemen vermeld die als "niet-blokkerend" worden bestempeld en die kunnen worden opgevangen door handmatige procedures of interventies, met name bij de toepassing van de voorbereiding van het stelsysteem en de injectie van verkiezingslijsten en lijsten van kandidaten.

Verkiezingen 2019 - Verslag van het College van Deskundigen

4.1.1.3 Opname van een correctie als gevolg van een probleem dat door de interne FOD is gedetecteerd vóór het voorverslag van het advies

Op 15 maart 2019, een week vóór het verslag van het adviesorgaan, ontdekte en rapporteerde FOD BiZa een probleem met de voorzittersmachines van de eerste generatie. Deze machines waren uitgerust met muizen die niet werden herkend door het systeem. SmartMatic was vergeten om deze op te nemen in het configuratiebestand van apparaten die op het systeem toegelaten waren.

De oplossing voor het probleem bestond erin om in een configuratiebestand op de voorzittersmachine een bestand toe te voegen. Deze informatie liet toe om de muis te herkennen en te aanvaarden als geautoriseerd apparaat.

Het bedrijf SmartMatic stelde een technische oplossing voor aan de FOD BiZa die het heeft voorgelegd aan het College. Deze laatste gaf een negatief advies over het ingediende voorstel, aangezien dit voorstel en de implementatie hiervan aanzienlijk en onnodig afweek van de gebruikelijke procedure voor het genereren van de "master" USB-sleutel. Daarom werd besloten om het probleem op niveau van de disk image van de voorzittersmachine te corrigeren en het configuratiebestand van de randapparatuur handmatig te verbeteren.

Op 25 maart 2019, in aanwezigheid van vertegenwoordigers van de FOD BiZa, het College van Deskundigen en het adviesorgaan, corrigeerden de vertegenwoordigers van het bedrijf SmartMatic de disk image van de voorzittersmachine door de vereiste correctie toe te passen op het configuratiebestand van de randapparatuur. Deze operatie werd uitgevoerd op de compilatie-pc en elke partij ontving een nieuw exemplaar van de compilatie-omgeving (kopie van de disk images voor de voorbereidingsomgeving, voor de voorzittersmachine en voor de stemmachine).

4.1.1.4 Aanmaak van de ECM voorbereidingsomgeving

Zoals hierboven besproken, bevat de SmartMatic-omgeving een basisomgeving voor het maken van USB-sleutels, waarvan kopieën op de verkiezingsdag in alle stembureaus worden gebruikt. Deze voorbereidingsomgeving omvat twee servers en een pc-client, alle drie verbonden op een geïsoleerd netwerk.

De "ECM" –disk image die tijdens de compilatie werd gegenereerd, wordt gebruikt om deze pc en deze twee servers te installeren en configureren.

Op 15 april 2019, in de gebouwen van de FOD BiZa, werd deze omgeving voor de voorbereiding van de USB-sleutel, "master key" genaamd, geïnstalleerd en gestart door de vertegenwoordigers van de FOD BiZa in aanwezigheid van leden van het College en vertegenwoordigers van het bedrijf SmartMatic.

De lijst met stemlokalen werd geladen in de "ECM" -omgeving en de verschillende cryptografische elementen die nodig zijn voor de verkiezingen werden gegenereerd. Het College nam er een kopie van.

Verkiezingen 2019 - Verslag van het College van Deskundigen

4.1.1.5 Aanmaak van de schermafdrucken

Na het afsluiten van de kandidaturen geregistreerd met behulp van Martine, werden de datasets met de kieslijsten en kandidatenlijsten geladen in de voorbereidingsomgeving ("ECM").

Dit gebeurde in aanwezigheid van het College op 24 april 2019

Vanuit deze omgeving wordt een specifieke USB-sleutel gegenereerd die op een stembus wordt gebruikt om schermafbeeldingen van lijsten en kandidaten te genereren. Deze schermafdrucken worden vervolgens ter goedkeuring voorgelegd aan de voorzitters van de hoofdbureaus.

4.1.1.6 Aanmaak van de "master key" voor de verkiezingen

Bij de goedkeuring werden opnieuw meer dan honderd verbeteringen gevraagd door de voorzitters van de hoofdbureaus om fouten te verbeteren die ze al ruim voordien hadden moeten detecteren.

Het risico op fouten is aanzienlijk. In deze fase van voorbereiding van de verkiezingen, betekent dat dat al deze correcties tweemaal moeten worden ingevoerd, eenmaal in de SmartMatic-omgeving en eenmaal in de Martine-omgeving.

Na deze correcties was de organiserende overheid in staat om de "master key" te genereren alsook de duplicatie ervan op meer dan 9000 USB-sleutels.

Het College heeft een kopie van de "master key" gemaakt om deze te gebruiken als referentie voor de na de verkiezingen uitgevoerde controles.

4.1.1.7 Aanmaak van de geheugendragers

Op 10 mei 2019 heeft het College de lokalen bezocht waar alle voor de verkiezingen gebruikte informatiedragers worden gedupliceerd. Het betreft de usb-sticks en de enveloppes met de wachtwoorden. De gang met alle lokalen waarin de informatiedragers worden aangemaakt, is beveiligd met een badgesysteem, een bewaker en camera's. De individuele lokalen voor de aanmaak worden afgesloten. Het personeel dat de USB sticks kopieert en de wachtwoorden uitprint, is in dienst van de FOD BiZa.

4.1.1.8 Testomgeving van het College

Het College beschikt over een testomgeving, bestaande uit virtuele machines voor de "ECM"- omgeving en heeft zijn eigen "master key" gegenereerd die het twintig maal heeft gedupliceerd om testen uit te voeren die op verschillende kantons betrekking hadden. Hiervoor beschikt het College over een voorzittersmachine en een stembus van de generatie '2018' waarmee het de volgende operaties heeft uitgevoerd:

- Openen van een stembureau (start urne en voorzittersmachine);
- Opstarten van stembussen;
- Het uitbrengen van stemmen en het bekijken van stemmen op de stemcomputer;

Verkiezingen 2019 - Verslag van het College van Deskundigen

- Decrypteren van ".VT" -bestanden met behulp van een door het College ontwikkelde software en vergelijking met de leesbare versie van de stem.

Al deze testen bleken op softwareniveau overtuigend te zijn.

Tijdens deze tests ontdekte het College een discrepantie in de taalversies van de stemmachinesoftware. Inderdaad, in de Franse en Duitse versie verschijnt aan het einde van de stemming een bericht waarin de kiezer wordt uitgenodigd om zijn stem te controleren met behulp van de handscanner die voor dit doel is voorzien in één stemhokje. In de Nederlandse versie verschijnt dit bericht niet.

Het College waarschuwde de FOD BiZa zodra dit werd ontdekt. Noch zij, noch het adviesorgaan hadden dit probleem opgemerkt. Spijtig genoeg was het gezien de laattijdigheid van deze ontdekking niet mogelijk om dit nog te verbeteren. De USB-sleutels waren reeds gegenereerd en onder omslag gestopt.

In een reactie liet de FOD BiZa mondeling weten dat de oorsprong van dit probleem in de bronbestanden van SmartMatic lag, dewelke duidelijk waren geïnspireerd op de configuratiebestanden die werden gebruikt voor de gemeentelijke en provinciale verkiezingen in Vlaanderen in 2018. De organiserende overheid van deze verkiezingen in Vlaanderen wenste deze vermelding, die de burger uitnodigde tot extra controle, niet meer te tonen.

4.1.2 Controles van het systeem Martine – module MA2X

Het bedrijf PwC heeft een mandaat gekregen voor het nagaan van de geschiktheid van het systeem Martine (overeenkomst PwC-Civadis van 26 februari 2019). De analyse werd beperkt tot de module MA2X en had betrekking op (1) veiligheid, de integriteit, de fraude en het geheim van de kiesprocedure, (2) conformiteit met de wetgeving, (3) functionaliteit en robuustheid van de systemen. PwC heeft heel wat geautomatiseerde controles uitgevoerd en heeft gesprekken gevoerd met het team belast met de ontwikkeling.

Op 17 mei 2019 woonde het College de voorstelling bij van het verslag van PwC betreffende hun evaluatie van MA2X (resultaatsverwerkingsmodule van Martine). Het College ontving op dat ogenblik ook het Franstalige verslag van PwC betreffende MA2X.

Met betrekking tot de andere vaststellingen bleek tijdens de voorstelling dat er over een belangrijk aantal daarvan ernstige meningsverschillen bestaan over de juiste interpretatie ervan tussen enerzijds PwC en anderzijds de leverancier CIVADIS. Tijdens de briefing werd overeengekomen om via schriftelijke weg CIVADIS de kans te bieden te reageren. Deze reactie zou verwerkt worden of toegevoegd aan het evaluatieverslag van PwC om tot een finale versie te komen.

Op het ogenblik van redactie van zijn verslag had het College dit bijgewerkt document nog niet mogen ontvangen.

Bij het verslag van PwC zijn volgende opmerkingen te maken:

- PwC heeft een aantal aspecten van het systeem niet onderzocht. (pag. 11-12 van hun verslag). Hieronder vallen onder meer de systemen gebruikt in de

Verkiezingen 2019 - Verslag van het College van Deskundigen

hoofdbureaus om de USB-sticks uit te lezen en/of de manueel getelde stemmen door te geven aan de centrale databank in Brussel. Zoals de ervaring heeft aangetoond zijn een aantal van die elementen wel degelijk belangrijk in bv. de betrouwbaarheid en de bruikbaarheid van het systeem.

- Er werd vastgesteld dat tot kort voor de verkiezingen er wijzigingen werden aangebracht aan de software (laatste versie 9 mei). Dit maakt een grondige screening van de software, zoals in de Kieswet voorzien, onmogelijk.

Uiteindelijk gaf PwC volgend advies: “Op basis van de door ons verrichtte werkzaamheden en op voorwaarde dat de nodige (bijkomende) uitbatingsinstructie(s) en/of manuele procedure(s) geïmplementeerd en uitgevoerd worden, en verwijzend naar de definitie van geschiktheid, besluiten wij met redelijke – maar geen absolute – zekerheid¹, dat de Toepassing “resultatenbeheer” (MA2X) beantwoordt aan de hierboven gedefinieerde criteria van geschiktheid”

4.1.3 Relaties tussen de bedrijven verantwoordelijk voor de ontwikkelingen

Om de authenticiteit en de betrouwbaarheid van de gegevens die worden uitgewisseld tussen SmartMatic en Martine systemen (ontwikkeld door Civadis) worden er verschillende computer technische mechanismen geïmplementeerd. Deze gegevens zijn nodig om de USB-sticks aan te maken en voor de berekening van de resultaten. De mechanismen zijn:

- Encryptie
- Elektronische handtekening
- Digitale vingerafdruk (hash-code)
- Checksum
- Etc.

De compatibiliteit van de twee systemen en een goede coördinatie tussen de twee bedrijven die verantwoordelijk zijn voor de ontwikkeling van software is essentieel. De FOD BiZa heeft het College op de hoogte gebracht van een aantal incidenten die de voorbereiding van de verkiezingen ontsierd hebben. De bedrijven SmartMatic en Civadis (Martine ontwikkelaar) verwezen naar elkaar wanneer er problemen optraden op vlak van compatibiliteit of bij de interpretatie van normen, standaarden en conventies die in hun software moesten worden geïmplementeerd.

Het College betreurt ten eerste de gebrekkige samenwerking tussen SmartMatic en Civadis.

4.1.4 Analyse van de broncode

Het College van Deskundigen heeft, gezien de korte duur van zijn opdracht, kort geanalyseerd hoe de computerbeveiliging in de verschillende systemen is geïmplementeerd, op basis van de broncode en technische documenten die van de bedrijven werden ontvangen. Het College van Deskundigen doet in dit verslag een

¹ Voor de term “redelijke zekerheid” werd verwezen naar het Koninklijk Besluit van 26 mei 2002 met betrekking tot systemen van interne controle binnen de federale overheidsdiensten (BS 31 lei 2002)

Verkiezingen 2019 - Verslag van het College van Deskundigen

reeks aanbevelingen met betrekking tot de veiligheid van stemsystemen en de implementatie van cryptografische technieken.

Het College van Deskundigen stelt ook maatregelen voor (op basis van systematische audits, systematische beoordelingen van stemmen door kiezers, kwaliteitsnormen voor broncodes en documentatie) om de transparantie en veiligheid van het volledige verkiezingsproces te verbeteren, ook in de periode vóórafgaande op de verkiezingen (ontwikkeling van broncode, generatie en beheer van cryptografische sleutels).

Het College van Deskundigen merkt op dat het soms moeilijk was om antwoorden te krijgen op vragen die aan het bedrijf SmartMatic werden gesteld.

4.1.5 Analyse door het CCB

4.1.5.1 Perimeter en methodologie

Het College van Deskundigen heeft specialisten van het Centrum voor Cyberveiligheid België (CCB) ontmoet en heeft de verschillende verslagen van het Centrum kunnen raadplegen.

De benadering van het CCB is op verschillende elementen gebaseerd :

- het beheer van de veiligheid op het niveau van de procedure ;
- de veiligheid van de ontwikkelingscyclus ;
- de aanbevelingen en het volgen ervan ;
- een oefening op het vlak van penetratie in het stelsysteem (pentesting).

Die analyses zijn in de praktijk uitgevoerd in de vorm van interviews, in voortdurende interactie met de bedrijven belast met de ontwikkeling van het stelsysteem (Civadis en SmartMatic) en/of ook op onafhankelijke wijze. Het organisatievermogen van de bedrijven wordt ook beoordeeld. De resultaten zijn voorgelegd en gerangschikt volgens de waarschijnlijkheid van het risico, de moeilijkheid van de uitvoering en tot slot de impact op de verkiezingen. Er werden veel correcties gevraagd bij Civadis en aan alle verzoeken werd voldaan.

In opvolging van de analyse die in 2018 werd uitgevoerd, is er een grote inspanning geleverd om de technische leiders van politieke partijen bewust te maken van de cyberbeveiliging van hun faciliteiten (websites, communicatiemiddelen) en crisis.

De CCB hielp ook met het opstellen van een DRP (disaster recovery plan) en het opstellen van formele procedures voor de beoogde incidenten.

Ingevolge die analyses en oefeningen, besluit het CCB dat de procedure verbeterd kan worden, maar dat het veiligheidsniveau van het geheel volstaat om verkiezingen in goede omstandigheden te organiseren.

4.1.5.2 Ontwikkelingscyclus en veiligheidsbeleid

Het CCB heeft een aantal interviews afgenomen en de documenten geanalyseerd die de bedrijven SmartMatic en Civadis bezorgd hebben.

Verkiezingen 2019 - Verslag van het College van Deskundigen

Het College van Deskundigen stelt in het algemeen vast dat het CCB de zwakke punten in kaart gebracht heeft die de bedrijven hadden kunnen opsporen en corrigeren vóór de start van de productie.

4.1.5.3 Veiligheid van de stemmachines en tellingsapplicatie “Martine”

Tijdens deze fase van de analyse heeft het CCB testaanvallen uitgevoerd op de het systeem (in modus “purple team”). Het CCB heeft op een aantal aandachtspunten gewezen. Die zijn voorgelegd aan de twee onderaannemers met het oog op bijsturing. Vervolgens is een vergadering georganiseerd om de genomen maatregelen te overlopen.

4.1.6 Bezoek aan het datacenter van FOD BiZa

Leden van het College zijn het datacenter van Martine gaan bezoeken op 9/5/2019. De servers bevinden zich in het serverlokaal van de FOD BiZa.

Het College heeft kunnen vaststellen dat alle best practises specifiek voor datacenters worden toegepast:

- persoonlijke veiligheid (beperkte en gecontroleerde toegang)
- netwerken (beschermd en redundant)
- voeding (gescheiden en redundant)
- database (in real time gedupliceerd en op 3 sites gedupliceerd)

4.1.7 Deelname aan de opleidingen

4.1.7.1 Opleiding van de opleiders

Het doel was om het gemeentepersoneel op te leiden, dat op zijn beurt de voorzitters en secretarissen van de stembureaus zou opleiden, gemeente per gemeente. Aangezien de opleiding van de opleiders plaatsvond in december 2018 en januari 2019 en het permanente College niet op de hoogte was, heeft het College deze opleidingen niet gevolgd.

4.1.7.2 Opleiding van de voorzitters van de stembureaus

De leden van het College volgden de opleidingen voor voorzitters en secretarissen van stembureaus van de volgende gemeenten:

- Aalst
- Anderlecht
- Sint-Agatha Berchem
- Berlare
- Brussel
- Eupen
- Lochristi
- Liedekerke
- Lubbeek
- Sint-Joost-ten-Node
- Sankt-Vith
- Sint-Lambrechts-Woluwe
- Sint-Pieters-Woluwe

Verkiezingen 2019 - Verslag van het College van Deskundigen

- Zele.

Globaal gezien vond het College de opleiding van een uitstekend niveau. Een aantal opmerkingen zijn echter op hun plaats:

- het afsluiten van een stembureau, met een overzicht van de procedures en in te vullen formulieren werd niet altijd uitgelegd. Als gevolg daarvan hadden veel stembureaus grote moeite om de formulieren in te vullen (Berlare, Zele);
- er was niet altijd demonstratiemateriaal beschikbaar (Sankt-Vith). De levering van demonstratiemachines zou kosten hebben veroorzaakt die niet voorzien waren in hun budget;
- sommige gemeenten hebben hun eigen documentatie (Berlare) opgesteld;
- een aantal demonstratiemachines leverde problemen op (Aalst, Lochristi);
- er wordt duidelijk gesteld (en herhaald) dat indien het kantoor om 7u30 niet is opgericht, de PC's nog steeds moeten worden opgestart (Anderlecht, Sint-Agatha-Berchem, Eupen), wat in strijd is met de wetgeving die het wachten op de oprichting van het kantoor vereisen;
- sommige locaties zijn niet voldoende ingericht: geen microfoon, te weinig banken om te noteren (Anderlecht, Sint-Agatha-Berchem);
- Het werd soms aangeraden om geen reclame te maken voor de handscanner om uw stem te controleren (Brussel).
- Soms was het demonstratiemateriaal wel aanwezig, maar de voorzitters van de stembureaus werden niet uitgenodigd om het te testen (Sint-Joost-ten-Node).
- Er werd tijdens de opleiding niet altijd gesproken over het correct loskoppelen van USB-sleutels van voorzitter machines (Liedekerke).

4.1.8 Naleving van de procedures

4.1.8.1 Bij de installatie van de ECM-omgeving

Bij de installatie van de ECM-omgeving (cfr 4.1.1.4) was het College zeer verbaasd te ontdekken dat een aantal verkiezingsconfiguratiebestanden pas op dit moment aan de FOD BiZa werden gegeven en dat ze niet aanwezig waren in de broncode die SmartMatic ter beschikking stelde voor de referentiecompilatie. Bovendien moesten sommige van deze bestanden nog worden aangepast om een aantal problemen aan te pakken die door de FOD BiZa waren geconstateerd en die niet werden ontdekt door de instantie van mening en / of als niet-blokkerend werden beschouwd.

Deze bestanden zijn ter goedkeuring voorgelegd aan het adviesorgaan.

Het College betreurt het dat er een procedureel verschil is tussen het formalisme van de referentiecompilatie (met kopiëren in aanwezigheid van getuigen, plaatsen in verzegelde enveloppen, plaatsen in de kluis, enz.) en het informeel overhandigen door het bedrijf SmartMatic van sommige configuratie- en zelfs programmeerelementen, die van invloed zijn op de werking van de voorzittersmachine en het gedrag van de stemmachine.

Verkiezingen 2019 - Verslag van het College van Deskundigen

4.1.8.2 Na het afsluiten van de indiening van de kandidaturen

Er werd aan het College gemeld dat, hoewel de lijsten werden opgesteld en gevalideerd door de voorzitters van de hoofdbureaus, sommigen nadat ze hun formele handtekening hadden gezet, nog steeds fouten ontdekten. Deze voorzitters eisten vervolgens dat zij deze lijsten konden verbeteren zonder de door de wetgeving opgelegde procedure na te leven.

Er zijn ongeveer honderd wijzigingen (spelling van namen van kandidaten, zoals het gebruik van geaccentueerde of niet-geaccentueerde tekens, namen van lijsten, ...).

In Antwerpen ontbrak de lijst 'Piratenpartij' (lijst 23) in het systeem Martine. De partij had zijn lijst correct ingediend, zoals de procedure bepaalt, maar men was ze vergeten toe te voegen. Een PV werd opgesteld voor dit probleem en in de definitieve tabel van Martine werden de ontbrekende gegevens toegevoegd.

Gezien de tijdslimieten voor de voorbereiding van geheugenmedia, dwongen deze last-minute vereisten de FOD BiZa- om deze wijzigingen met spoed buiten de procedure en wettelijke bepalingen uit te voeren, wat de oorzaak van de fouten kan zijn geweest.

4.2 Vaststellingen op de verkiezingsdag

Op de verkiezingsdag hebben de leden van het College controles verricht in de stembureaus en in de totalisatiebureaus.

4.2.1 Controles in de stembureaus

De deskundigen hebben controles verricht in een aantal stembureaus waar elektronisch gestemd werd. Het betrof voornamelijk drie soorten controles: het uitbrengen van teststemmen voor latere analyse, een bevraging van de leden van het Bureau op basis van een standaardvragenlijst, het verloop van de verrichtingen observeren.

4.2.1.1 Teststemmen

In elk gecontroleerd stembureau werden teststemmen uitgebracht door de deskundigen van het College, vaak in aanwezigheid van de voorzitter of een door de voorzitter van het stembureau aangewezen bijzitter. De bijzitter en de deskundige hebben samen de uitgebrachte stemmen gecontroleerd in het stemhokje dat voorzien was voor de visualisatie van de stem. Alle stemmen werden getrouw weergegeven op het scherm.

De biljetten werden vervolgens meegenomen door de deskundige om te worden onderzocht in de eigen omgeving van het College na de verkiezingsdag.

4.2.1.2 Vragenlijst

Vervolgens werd door de deskundige een verslag opgesteld op grond van een standaardvragenlijst, in samenwerking met de voorzitter van het stembureau. Daarin werden de eventuele incidenten opgetekend. Dat verslag werd opgesteld om de moeilijkheden op te sporen en diensgevolge aanbevelingen voor te stellen.

Verkiezingen 2019 - Verslag van het College van Deskundigen

4.2.1.3 Gecontroleerde stembureaus

De gecontroleerde stembureaus worden vermeld in onderstaande tabel.

Kanton	Gemeente	Stembureau
Aalst	Aalst	5,6,8,61,65
Aalter	Aalter	1,4,5,14
Asse	Affligem	28,31
Sankt Vith	Amel	11,12,13,14
Hoogstraten	Baarle-Hertog	16
Zelee	Berlare	18
Bilzen	Bilzen	16
Puurs-Sint-Amands	Bornem	14
Brussel	Brussel	12,13,15,25,26,28,29
Sankt Vith	Bullingen	16,17,18
Sankt Vith	Burg Reuland	19,20,21
Sankt Vith	Bütgenbach	22,23,24,25,27
Deinze	Deinze	1,3
Asse	Dilbeek-Schepdaal	45,68
Brugge	Dudzele	112
Sankt Vith	Elsenborn	22
Elsene	Elsene	4,13,48,51
Sint-Joost-Ten-Node	Etterbeek	13,17,24
Eupen	Eupen	1,3,8,9,10
Lennik	Gaasbeek	4
Sint-Jans-Molenbeek	Ganshoren	55
Zoutleeuw	Geetbets	12,14
Glabbeek	Glabbeek	5
Hasselt	Hasselt	8,11,57,58
Leuven	Herent	95
Sint-Jans-Molenbeek	Jette	73, 82
Brecht	Kalmthout	45
Eupen	Kelmis	17,18,19,20
Brugge	Knokke-Heist	182
Sint-Jans-Molenbeek	Koekelberg	104
Veurne	Koksijde	42
Kortrijk	Kortrijk	17,18,20,55,61
Sint-Genesius-Rode	Kraainem	26
Lennik	Lennik-Gaasbeek	8
Leuven	Leuven	2,11,160,78,69
Zoutleeuw	Linter	24
Lochristi	Lochristi	11
Eupen	Lontzen	21,23,24,25
Oostende	Oostende	64
Elsene	Oudergem	57, 62, 77
Eupen	Raeren	27,29,30
Roeselare	Roeselare	42, 44

Verkiezingen 2019 - Verslag van het College van Deskundigen

Saint-Gilles	Saint-Gilles	18
Sankt Vith	Saint-Vith	5,6,7,8,17
Schaarbeek	Schaarbeek	62
Anderlecht	Sint-Agatha-Berchem	78
Sint-Jans-Molenbeek	Sint-Jans-Molenbeek	21,43
Sint-Joost-Ten-Node	Sint-Joost-Ten-Node	1,2,3,9,10,11,12
Sint-Joost-Ten-Node	Sint-Lambrechts-Woluwe	67
Sint-Truiden	Sint-Truiden	17,18,20
Asse	Ternat	115
Tongeren	Tongeren	22
Veurne	Veurne	7
Voeren	Voeren	1
Elsene	Watermaal-Bosvoorde	94,95, 96
Sint-Genesius-Rode	Wemmel	45
Sint-Genesius-Rode	Wezembeek	54
Sint-Joost-Ten-Node	Sint-Pieters-Woluwe	99
Zoutleeuw	Zoutleeuw	3,9

4.2.2 Incidenten in de stembureaus

4.2.2.1 Procedure

4.2.2.1.1 Diversen

Beschrijving

- het openen van de enveloppen met de wachtwoorden en USB-sleutels vooraleer het bureau volledig was samengesteld;
- niet verzegelde kleppen die de USB-poorten in de stemmachines beschermen;
- niet-verzegelde urne;
- geen controle van de teststemmen door de QR-lezer in het stemhokje;
- enveloppen met de USB-sleutels en de paswoorden in de stembureaus neergelegd;
- ontbreken van teststemmen.

Oplossing

Opvolgen van de instructies in de handleiding.

4.2.2.1.2 USB sleutels gekoppeld aan de voorzittersmachine

Beschrijving

Tijdens de controle van het stembureau bleek dat de USB-sticks niet gekoppeld aan de urne waren, maar gekoppeld aan de voorzittersmachine.

Oplossing

Eerst werd één USB-sleutel correct verwijderd en terug gekoppeld aan de urne. Vervolgens werd de tweede USB-sleutel correct verwijderd en de voorzitter heeft deze USB-sleutel ook gekoppeld aan de urne.

Verkiezingen 2019 - Verslag van het College van Deskundigen

In de configuraties "voorzittersmachines en urnen die erop verbonden zijn", heeft het College nagegaan dat alle USB-poorten onderling uitwisselbaar zijn en geen invloed hebben op de goede werking van het systeem.

4.2.2.1.3 Specifiek vertaalprobleem voor de verkiezingen in de Duitstalige Gemeenschap

De Duitse vertaling van de documenten "ACEG/11bis" en "Handleiding voor de voorzitters van de stembureaus met elektronische stemming met papieren bewijsstuk" houdt geen rekening met het feit dat er 4 verkiezingen zijn in de Duitstalige kantons.

Het Duitstalige PV, aangemaakt door MA2X, is niet aangepast aan het huidige systeem voor elektronisch stemmen. Er wordt bijvoorbeeld gesproken over diskettes.

4.2.2.2 Materialen

4.2.2.2.1 Voorbeelden

Overzicht technische problemen:

- niet werkende USB-sleutels;
- problemen bij het opstarten van de voorzittersmachine;
- herstarten nadat USB-sleutels niet in orde zijn;
- problemen bij het verwijderen van de USB-sleutels uit de stemmachine;
- storing van het aanraakscherm van een stemmachine;
- panne van een stemmachine;
- storing van de voorzittersmachine;
- printerstoring;
- problemen met het afdrukken van papieren bewijsstukken;
- probleem met lezen van de stemmen door de urne.

4.2.2.2.2 Oplossing

Bij problemen met apparatuur van het stemlokaal, was SmartMatic contractueel verantwoordelijk voor het vervangen van defecte apparatuur binnen een bepaalde tijdslimiet, afhankelijk van het type defect. De vervangende USB-sticks werden geleverd binnen de tijdslimiet van 30 minuten wanneer het om blokkerende punten ging, wat hier het geval was.

4.2.2.3 Andere

4.2.2.3.1 Printerstoring van de stemmachine en dubbele stemmen

Beschrijving

In de printer van sommige stemmachines werden stembiljetten geblokkeerd. De betrokken kiezers konden opnieuw stemmen in een ander stemhokje.

Tijdens de interventie van de technicus werd het stembiljet - of de nog aan elkaar hangende stembiljetten - in de stemmachine terug gevonden. Dit stembiljet of deze stembiljetten werden soms verkeerdelijk gescand en in de urne geworpen door een

Verkiezingen 2019 - Verslag van het College van Deskundigen

lid van het bureau, waardoor de twee stembiljetten van de betrokken kiezers werden ingelezen (Sint-Gillis 18).

Oplossing

Stembureaus moeten de instructie krijgen om nooit in de stemmachines geblokkeerde stembiljetten te scannen, anders is er sprake van dubbele stemmen. Deze stembiljetten moeten als nietig worden beschouwd en als zodanig worden behandeld.

*4.2.2.3.2 Bulletins die in de urne worden geworpen zonder gescand te zijn.***Beschrijving**

Bij de hertelling van de urnen in de kantonhoofdbureaus bleek dat het aantal gescande stemmen hoger was dan in het kerncijferrapport van het stembureau was aangegeven. Na analyse is de enige aannemelijke verklaring dat sommige stembiljetten in de urne werden geworpen zonder te zijn gescand.

4.2.3 Controles in de hoofdbureaus

Leden van het College bezochten de volgende hoofdbureaus op verkiezingsavond:

- Antwerpen
- Sint-Agatha-Berchem
- Brussel
- Eupen
- Leuven
- Lennik
- Malmedy
- Sint-Gillis
- St. Vith
- Tongeren
- Zaventem

Een overgrote meerderheid pc's in de hoofdbureaus ondervonden problemen bij het verbinden met de Martine-omgeving (zie 4.2.5.2.). De helpdesk was niet of nauwelijks bereikbaar.

Het College van Deskundigen heeft, dit probleem terzijde, een zekere “vrijheid” vastgesteld in de manier van bezorgen van de USB-sticks aan de kantonhoofdbureaus (enveloppen soms niet-ondertekend, soms niet-verzegeld, soms zelfs zonder verpakking).

Evenzo werden sommige hertellingen uitgevoerd in de hoofdbureaus, met een zeker tijdsverlies als enig gevolg.

4.2.4 Incident : Voortijdige publicatie van resultaten op de websites van de media**Vaststelling**

Verkiezingen 2019 - Verslag van het College van Deskundigen

Op de verkiezingsdag werd rond 15u30 vastgesteld dat er eerste resultaten (een bureau uit Tongeren) werden gepubliceerd terwijl de verkiezingen nog liepen.

Bij navraag door leden van het College bij het betreffende hoofdbureau bleek dat de resultaten wel degelijk overeen kwamen met de resultaten van de manuele telling. Uit gesprekken met de leden, en in het bijzonder de voorzitter van het Bureau, kon worden besloten dat:

- De resultaten nog niet waren ingegeven in Martine;
- Het Bureau bezoek had gehad van journalisten.

Uit contact met de verantwoordelijke van FOD BiZa bleek tevens dat er nog geen enkel resultaat werd doorgestuurd via Martine, dit werd bevestigd door de website van FOD BiZa waar geen resultaten werden vermeld.

Er werd tevens vastgesteld dat het systeem Martine pas om 16:40 de eerste resultaten doorstuurde naar de media.

Conclusie

Het voortijdige verspreiden van resultaten van het eerste bureau in Tongeren gebeurde buiten de officiële kanalen om door journalisten ter plaatse en valt buiten bevoegdheid van het College.

De bevestiging door FOD BiZa dat er geen resultaten werden verspreid voor 16u en de bevestiging daarvan via de sftp-server doen redelijkerwijze vermoeden dat ook andere vroegtijdig gepubliceerd resultaten werd verkregen buiten de officiële kanalen om.

4.2.5 Incidenten met het doorsturen van de resultaten door de kantons op de avond van de verkiezingen

4.2.5.1 Samenvatting en impact op het resultaat van de verkiezingen

De procedure voorziet dat de elektronische resultaten (op de USB-sleutels van de voorzitters-machines of manuele PV's in het geval van een papieren stemming) worden doorgestuurd van de hoofdbureaus naar het MARTINE-systeem.

Kort nadat de eerste gegevens werden verzonden, bleek dat een grote meerderheid van de kantons zich niet meer konden aanmelden op het systeem. Het systeem was enkele uren niet beschikbaar (van 16.00 tot 20.10 uur).

Na analyse van de aan de aan het College bezorgde informatie kon het concluderen dat dit incident geen invloed heeft gehad op de verkiezingsresultaten.

4.2.5.2 Technische beschrijving van de incidenten op basis van de aan het College bezorgde informatie

4.2.5.2.1 Incident 1 – Geblokkeerde toegang tot het systeem om resultaten door te sturen

Het incident begon rond 16.00 uur. Verschillende bureaus hebben de Civadis-helphdesk gebeld om te melden dat het onmogelijk was om verbinding te maken met

Verkiezingen 2019 - Verslag van het College van Deskundigen

de MA2X-modules. De modules, firewall, load-balancer en databases bleven correct reageren en de verschillende parameters leken normaal. Het was echter niet mogelijk om nieuwe verbindingen met de systemen tot stand te brengen. Na analyse van de verschillende elementen (Proximus-netwerk en -routers, firewallregels, enz...), bleek dat er een aanzienlijk aantal DNS-sessies open waren op de Martine firewall. Deze sessies waren te wijten aan de (privé) DNS-server die door de clients (PC in de hoofdbureaus) werd gebruikt en die was geconfigureerd om te voorkomen dat andere sites dan de voor Martine toegestane sites werden opgezocht. Volgens de eerste analyses waren dit een groot aantal updatecontroles door het operatingssysteem (Windows 7) van de computers en de routers die, door Civadis, ter beschikking van de hoofdbureaus werden gesteld om de resultaten in te geven en door te sturen.

Er werd beslist om de DNS-verzoeken die door de Martine-infrastructuur worden verwerkt om te leiden naar de DNS-servers van FOD BiZa. De open sessies werden daardoor geleidelijk aan weggewerkt.

4.2.5.2.2 Incident 2 – Verbroken verbinding via het Publilink netwerk

Nadat het eerste incident was opgelost, bleven er toegangsproblemen bestaan. Nieuwe sessies konden niet worden gestart en verbroken sessies konden niet worden hersteld.

Uit een analyse bleek dat het niet mogelijk was om via het Publilink netwerk de servers van Martine te bereiken, terwijl dit wel mogelijk was via het internet of het FOD BiZa-netwerk. De support van Martine stelde vervolgens voor om de toegang tot de MA2X-module om te schakelen van Publilink naar Internet/Fedman (op het BELNET-netwerk). De oplossing werd wat veiligheid betreft gevalideerd door de ingenieurs van de CCB en CERT die bij FOD BiZa aanwezig waren.

Op dat moment werd de verbinding hersteld en werd het verzenden van de resultaten normaal hervat.

4.2.5.2.3 Incident 3 – blokkerende filter op de firewall van FOD BiZa

In de late avond werden, door een toevoeging van een filterregel op de FOD BiZa firewall de actieve verbindingen verbroken, met een groot aantal oproepen naar de helpdesk als gevolg. De regel werd geschrapt, waarna verder gewerkt kon worden.

4.2.5.2.4 Opvolging van de incidenten en besluit

Op maandag 27 mei vroeg het College aan de directeur-generaal van FOD BiZa om een volledige analyse van de gebeurtenissen van de vorige dag, een opvolging van de beslissingen die genomen werden op de crisisvergaderingen en om de logs van de verschillende elementen te verzekeren voor verdere analyse. FOD BiZa is een intern onderzoek gestart en heeft volledig op transparante en snelle wijze meegewerkt met het College.

Het College kon op basis van de ontvangen informatie en de analyses die zij heeft uitgevoerd, besluiten dat de IT-problemen slechts tot vertragingen in het proces hebben geleid. Cryptografische eigenschappen (integriteit van de stemresultaten, authenticiteit van de verzendbronnen in Martine, vertrouwelijkheid van de

Verkiezingen 2019 - Verslag van het College van Deskundigen

communicatie) werden gedurende het hele proces gegarandeerd. Ze zijn in overeenstemming met wat er verwacht wordt van het elektronische stem- en datatransmissiesysteem Martine.

Het College kon ook het DRP (disaster recovery plan) van het CERT / CCB, de procedures voor crisismanagement en de technische analyses van het CERT / CCB onderzoeken.

4.3 Na de verkiezingsdag uitgevoerde controles

4.3.1 Verificatie van de totalisaties

Net als bij de verkiezingen van 2014, en in het bijzonder na de problemen die werden ontdekt tijdens de verkiezingen van 2018², wilde het College opnieuw een volledige hertotalisatie uitvoeren van de stemmen aanwezig op de geheugendragers die in de stembureaus werden gebruikt.

Het doel was om de resultaten, bekomen door het College met behulp van zijn eigen software, te vergelijken met de gegevens die Martine op de verkiezingsavond in de media en op de officiële verkiezingswebsite <https://verkiezingen2019.belgium.be/> verspreidde.

4.3.1.1 Verzameling van de USB-sticks

Om door te gaan met de hertotalisatie moest het College alle USB-sleutels verzamelen die op de dag van de verkiezingen werden gebruikt. Hiertoe heeft de FOD BiZa een richtlijn gestuurd naar alle kantonbureaus waar de elektronische stemming wordt gebruikt waarin gevraagd werd om alle USB-sleutels in het kieskringhoofdbureau A (voor de Kamer) te verzamelen vóór maandag 27 mei 15.00 uur.

Helaas is deze richtlijn niet door alle kantonvoorzitters gelezen. Bovendien werd in sommige kantons geen procedure ingevoerd om de sleutels te verzamelen. Hierdoor was het niet mogelijk om alle sleutels te bemachtigen. Uiteindelijk ontbraken in totaal 3 sets USB-sleutels uit 3 verschillende kantons.

4.3.1.2 Lezen van de USB-sticks

Het College heeft een specifieke informaticaomgeving (besturingssysteem, software) opgesteld om een kopie te nemen van de gegevensdragers die tijdens de stemming in de stembureaus zijn gebruikt, te analyseren en te verwerken.

Met behulp van die omgeving, heeft het College kopieën genomen van alle USB-sticks van alle stembureaus die in de hoofdbureaus werden gebruikt voor de telling. Het heeft ook kopieën genomen van de USB-sticks die werden gebruikt voor verschillende hertellingen in verschillende gemeenten. Tot die hertellingen werd in de hoofdbureaus beslist om verscheidene redenen, zoals o.a. het scannen van de

² in een Brusselse en in een zestal Vlaamse gemeentes had een menselijke manipulatiefout de sluiting van het stelsysteem verstoord, met als resultaat dat niet alle stemmenbiljetten werden geteld.

Verkiezingen 2019 - Verslag van het College van Deskundigen

referentiestemmen van het stembureau of het annuleren van stembiljetten die waren gescand, maar niet in de urne gedeponeerd.

4.3.1.3 Verificatie en decryptie van de USB-sticks

Door middel van de omgeving van het College voor het kopiëren van de gegevensdragers konden diverse controles automatisch worden uitgevoerd:

- vergelijking van de inhoud van de twee sticks van hetzelfde bureau ;
- vergelijking van de software voor de verwerkingssystemen, uitvoerbare programma's en datasets (gemeenten, lijsten, kandidaten enz.) met die van een referentie-USB-stick ;
- verificatie en decryptie van de ".VT"-bestanden op de sticks.

Het College heeft geen enkele onregelmatigheid vastgesteld bij de verzamelde sticks en is overtuigd van hun echtheid. Dankzij de geldende procedures en cryptografische beveiligingen kan het eveneens besluiten dat het wel degelijk om de authentieke USB-sticks gaat die in de verschillende stembureaus werden gebruikt bij de verkiezingen.

Met behulp van een softwaretool geleverd door SmartMatic (en waarvan de broncode beschikbaar is) en de verschillende wachtwoorden ontvangen van de FOD BiZa, is het College overgegaan tot het decrypteren van alle ".VT" type bestanden in haar bezit.

Het College was dus in staat om voor elk stembureau (waarvan zij ten minste één sleutel had) de gedecrypteerde ".VT"-bestanden te verkrijgen.

Gezien de cryptografische systemen en de geldende digitale handtekeningen die van kracht zijn in het systeem, evenals de foutloze decryptie van alle ".VT" -bestanden, is het College overtuigd van de echtheid van de stemmen die opgeslagen werden op de USB-sticks.

4.3.1.4 Kopieën van de ".VT"-bestanden voor de ontbrekende sleutels

Wanneer de USB-sticks in het hoofdbureau van het kanton worden ingelezen om de resultaten te verzamelen, haalt het Martine-systeem ook de ".VT"-bestanden op en slaat ze op een centrale server op.

Om de ontbrekende USB-sticks in 3 kantons te compenseren, heeft het College bij Civadis, via de FOD BiZa, een kopie gevraagd en verkregen van de ".VT"-bestanden die op de verkiezingsavond door het Martine-systeem zijn opgenomen.

Deze bestanden werden gedecrypteerd met behulp van de wachtwoorden van het stembureau waar ze werden gecreëerd.

Gezien de cryptografische en digitale ondertekening in het systeem en de foutloze decryptie van deze ".VT"-bestanden, is het College overtuigd van hun authenticiteit.

Verkiezingen 2019 - Verslag van het College van Deskundigen

4.3.1.5 Volledige hertelling van de USB-sticks per gemeente

Zodra de “.VT”-bestanden gedecrypteerd waren, heeft het College eigen ontwikkelde software gebruikt om een volledige nieuwe totalisatie van alle “.VT”-bestanden uit te voeren voor alle stembureaus van alle gemeenten.

4.3.1.6 Capteren van de naar de media verspreide resultaten

Met het oog op het capteren van de gepubliceerde resultaten schreef het College zich in in de procedure zoals voorzien voor de Media. Dit impliceerde het opzetten van een SFTP-server (beveiligde fileserver) waarop FOD BiZa via het systeem Martine periodiek de tussentijdse en, van zodra beschikbaar, de definitieve resultaten, bezorgt.

Dit liet niet alleen toe om de resultaten te capteren maar tevens op te volgen op welk tijdstip welke resultaten verstuurd werden.

De ontvangen bestanden werden door middel van eigen software opgeslagen in een lokale databank met oog op de vergelijking met de resultaten zoals bekomen na de hertelling (Cfr. hierboven).

4.3.1.7 Controle van de hertotalisatie

Op basis van de aldus verkregen totalen heeft het College verschillende verificaties uitgevoerd, zowel van de kiescijfers als van de voorkeur- en blanco stemmen zoals gepubliceerd op de officiële website van de verkiezingen. Het College heeft tijdens deze controles geen discrepanties ontdekt.

Bovendien werd voor alle verkiezingen een geautomatiseerde en volledige vergelijking gemaakt op het niveau van de resultaten per gemeente, zowel op het niveau van het verkiezingscijfer van elke lijst als op het niveau van de voorkeurstemmen van elke kandidaat en de lijststemmen.

Ook hier vond het College geen verschil tussen de hertotalisatie en de gegevens die door het systeem Martine worden verspreid.

4.4 Verspreiding van de broncode**4.4.1 Broncode van de SmartMatic-software**

Het College heeft kunnen vaststellen dat de broncode van de software werd bekendgemaakt op de officiële verkiezingssite.

Het College heeft die bronnen vergeleken met die, welke het verkregen heeft van SmartMatic en die gebruikt werden bij de referentiecompilatie om de programma's te maken die op de verkiezingsdag werden gebruikt. De bekendgemaakte broncode is dezelfde als die, welke van SmartMatic komt.

4.4.2 Broncode van het systeem Martine

De wet voorziet niet in de vrijgave van de broncode van het systeem Martine.

5 Aanbevelingen

5.1 Aanbevelingen ten gevolge van het probleem met het doorsturen van de resultaten

[#2019-BE.1] Het College beveelt aan om het "disaster recovery plan" te herzien door systematisch rekening te houden met de impact van elke dienst van derden (DNS, authenticatie via eID, enz.).

[#2019-BE.2] Het College beveelt aan om de machines, die in de hoofdbureaus gebruikt worden om gegevens te versturen, te updaten en onnodige toegang tot deze machines zoveel mogelijk te beperken (bijvoorbeeld door middel van een software firewall).

[#2019-BE.3] Het College beveelt aan om enkele weken voor de verkiezingen verschillende geautomatiseerde tests uit te voeren op de huidige (niet gesimuleerde) infrastructuur. Deze tests moeten onder andere de grenzen van de infrastructuurbelasting in reële omstandigheden testen en het mogelijk maken om na te gaan in hoeverre het noodherstelplan voldoet.

[#2019-BE.4] Het College beveelt aan dat het proces wordt ontworpen alsof de gegevens systematisch over een onbeveiligd openbaar netwerk worden verzonden.

[#2019-BE.5] Het College beveelt aan om PwC's missie uit te breiden met de analyse van transmissiecomputers in de kantonhoofdbureaus.

5.2 Aanbevelingen betreffende de procedures

[#2019-BE.6] Tijdens haar controles in de stemlokalen heeft het College vastgesteld dat veel voorzitters van stemlokalen problemen ondervonden met de sluiting van het stemlokaal (in te vullen formulieren, te gebruiken enveloppen, enz.).

[#2019-BE.7] Het College van Deskundigen beveelt aan om het beheersplan voor incidenten te actualiseren, met onder andere duidelijke procedures voor incidenten die voor, tijdens of na de verkiezingsdag zouden voorvallen.

[#2019-BE.8] Het College van Deskundigen beveelt aan de inhoud van de USB-sticks systematisch te wissen na de verkiezingen.

[#2019-BE.9] Het College van Deskundigen beveelt aan in de procedures een duidelijke, nominatieve en nauwkeurige identificatie te voorzien van de personen die tussenkomen in de stembureaus en in de hoofdbureaus bij de verkiezingen, in het bijzonder van de technici.

[#2019-BE.10] Het College van Deskundigen beveelt aan dat het tekstgedeelte van het stembiljet ook het lijstnummer bevat, evenals de naam van het kanton of de gemeente waarin de stem werd uitgebracht.

Verkiezingen 2019 - Verslag van het College van Deskundigen

[#2019-BE.11] Het College van Deskundigen beveelt aan de kiezers te informeren en te verzoeken om de leesbare en de gecodeerde versie van de stem die zij hebben uitgebracht te vergelijken voordat die gedigitaliseerd en in de urne gestoken wordt.

[#2019-BE.12] Het College van Deskundigen beveelt aan dat de broncodes voldoen aan de hoogste kwaliteitseisen en -criteria inzake methoden voor veilige softwareontwikkeling.

[#2019-BE.13] Het College van Deskundigen beveelt aan dat de software voor het geautomatiseerd stelsysteem wordt ontwikkeld met gestandaardiseerde ontwikkelingsinstrumenten in een duidelijke, leesbare en van relevante commentaar en documentatie voorziene code. Alle procedures en specificaties die het mogelijk maken om de uitvoeringsbestanden te produceren moeten duidelijk beschreven en gemakkelijk gereproduceerd kunnen worden (aanbeveling #2012-BXL.20). Alle programma's, bibliotheken, de versies en uitvoeringsparameters ervan moeten nauwkeurig worden gedocumenteerd. Het betreft het toepassen van de goede ontwikkelingspraktijken.

[#2019-BE.14] Met het oog op de vastgestelde tekortkomingen inzake de naleving van de procedures, beveelt het College van Deskundigen aan een systematische controle uit te voeren om zich ervan te vergewissen dat alle procedures worden toegepast.

[#2019-BE.15] Het College van Deskundigen beveelt aan om zijn aanbevelingen grondig te lezen, in het bijzonder [#2019-BE.15].

[#2019-BE.16] Het College van Deskundigen beveelt aan de MD5- of SHA-1-algoritmes niet meer te gebruiken, maar over te stappen op SHA-2 (SHA-512) of SHA-3.

[#2019-BE.17] Het College van Deskundigen beveelt aan de code van het SmartMatic-systeem op te schonen om elke ongebruikte code in het kader van de verkiezingen in België te vermijden.

[#2019-BE.18] Het College van Deskundigen beveelt aan dat het aantal pogingen om een wachtwoord in te geven wordt beperkt en dat de FOD BiZa een duidelijk en gedocumenteerd beleid op touw zet voor wat er gebeurt wanneer het maximumaantal pogingen wordt overschreven (wachtermijn alvorens opnieuw te kunnen beginnen of uitsluiting).

[#2019-BE.19] Het College van Deskundigen dringt erop aan de volledige resultaten van de verkiezingen beschikbaar te stellen op de officiële website van de verkiezingen in een "open data"-formaat (JSON, CSV...) om de controles te vergemakkelijken.

5.3 Aanbevelingen naar aanleiding van de verslagen van de CCB

Na het lezen van de verslagen van de CCB doet het College de volgende aanbevelingen.

Verkiezingen 2019 - Verslag van het College van Deskundigen

[#2019-BE.20] Het College van Deskundigen beveelt aan het crisisplan te verbeteren, zowel op het gebied van hardware- als software-infrastructuur, en deze aan te vullen met een communicatieplan en/of een "disaster recovery plan".

[#2019-BE.21] Het College van Deskundigen beveelt aan om Martine op een veilige manier te ontwikkelen, zonder te wachten tot het CCB zijn oefeningen aan het einde van de ontwikkelingscyclus uitvoert.

[#2019-BE.22] Het College van Deskundigen beveelt aan dat AES-codering niet langer wordt gebruikt in CBC-modus voor authenticatie.

[#2019-BE.23] Het College van Deskundigen beveelt aan om de systeemdokumentatie te genereren en te onderhouden gedurende de gehele ontwikkelingscyclus en niet alleen aan het eind van de ontwikkelingscyclus.

[#2019-BE.24] Het College van Deskundigen beveelt aan om de leveringskanalen van USB-sticks en wachtwoorden te scheiden.

[#2019-BE.25] Het College van Deskundigen beveelt de implementatie aan van een cryptografisch sleutelgeneratieproces dat niet gevoelig is voor het "sleutel escrow-probleem" (afpersing van sleutels door de persoon die ze genereert).

[#2019-BE.26] Het College van Deskundigen beveelt aan om de beveiligingsimpact van de onderlinge afhankelijkheid van software (externe of open source bibliotheken) en oproepen aan derden (bv. voor authenticatie of DNS) beter te beoordelen.

[#2019-BE.27] Het College van Deskundigen beveelt aan om een systeem van sondes (IDS) in te voeren om ongewenst verkeer op het netwerk op te sporen (anders dan dat wat strikt noodzakelijk is voor verkiezingen) en om een procedure in te voeren om ongewenst verkeer op te ruimen.

[#2019-BE.28] Het College van Deskundigen beveelt aan dat de systemen die in de kantonhoofdbureaus worden gebruikt voor de verzending van de resultaten moeten bestaan uit een vrije, veilige en "hardened" besturingssysteem en software, zoals dat ook het geval is voor de systemen die in de stembureaus worden gebruikt.

5.4 Algemene aanbevelingen

[#2019-BE.29] Het College van Deskundigen beveelt aan de interface schermen te laten doorlichten door ergonomie

[#2019-BE.30] Het College van Deskundigen beveelt aan dat elk bestand dat door de organiserende autoriteit openbaar wordt gemaakt met betrekking tot de verkiezingen (resultaten, broncode, enz.), gepubliceerd wordt met een hash en bijbehorende elektronische handtekening. Het College van Deskundigen beveelt aan dat deze documenten permanent beschikbaar zijn op een site met een zoekfunctie.

[#2019-BE.31] Het College van Deskundigen vraagt dat de wetgeving betreffende het elektronisch stemmen zodanig wordt gewijzigd dat de gebruikte

Verkiezingen 2019 - Verslag van het College van Deskundigen

geheugendragers ten laatste om 15.00 uur, de dag na de verkiezingen, aan het College bezorgd wordt.

[#2019-BE.32] Het College dringt erop aan dat alle configuratie- en programmeerelementen aanwezig zijn in de broncode die door SmartMatic wordt verstrekt tijdens de referentiecompilatie.

6 Besluit

Na de wijziging van de wetgeving is het College nu bevoegd om de elektronische stelsystemen te controleren, maar ook "alle software die bij de verkiezingen wordt gebruikt, zelfs wanneer er op andere manieren wordt gestemd dan op grond van deze wet". De missie van het College wordt dus uitgebreid tot het computersysteem dat wordt gebruikt in gemeenten en kantons met behulp van de traditionele "papier" stem.

Zoals eerder richtte het College zijn werk voornamelijk op de elementen die alleen zij wettelijk konden controleren (zoals de hertotalisatie van geheugenmedia die worden gebruikt in elektronische stembureaus). Daarom heeft het College de resultaten van het tellen en de totalisatie voor de traditionele stemming niet uitgebreid onderzocht, aangezien de democratische controle in de telbureaus en in de betrokken kantonbureaus wordt gewaarborgd door de geldende wettelijke bepalingen.

Binnen de grenzen van de missie, de middelen en de beschikbare tijd, concludeert het College als volgt:

- Voor de gemeentes en kantons die gebruik maakten van het elektronisch stemmen, vond het College geen enkel verschil tussen de gepubliceerde resultaten die door Martine aan de media werden gecommuniceerd en die werden gepubliceerd op de officiële website van de verkiezingen en de exhaustieve totalisaties van het College die bekomen werden op basis van de USB-sleutels. Het College besluit daarom dat de systemen de stemmen voor deze kantons en gemeenten correct hebben verzameld en getotaliseerd
- Voor gemeenten die traditionele stemmen, heeft het College niet gehoord van problemen, fouten en / of inconsistenties in de resultaten die zijn ingegeven op basis van de PV's van de totalisatiebureaus en de PV's van de kantonbureaus. Het is van mening dat dergelijke problemen, fouten en / of inconsistenties door deze bureaus zelf kunnen worden opgespoord.

Het College is daarom van mening dat het probleem van het verzenden van de resultaten op de verkiezingsnacht geen invloed heeft gehad op de resultaten van de verkiezingen.

Het College is tevens van mening dat het geïmplementeerde doel, zijnde het uitbrengen van stemmen, deze opnemen en tellen volgens de wettelijke bepalingen werd bereikt.

Het College dankt alle betrokkenen, met wie het heeft gewerkt tijdens zijn controlemissie, voor hun samenwerking: de vertegenwoordigers van de bedrijven, het adviesorgaan en de CCB, de leden van de stembureaus en de hoofdbureaus, alsmede het personeel van de gemeenten.

Zij wil in het bijzonder de vertegenwoordigers van de FOD BiZa bedanken voor hun uitstekende samenwerking, hun beschikbaarheid en hun reële verlangen naar transparantie, in het bijzonder bij het analyseren van het probleem bij het versturen van de resultaten.

Verkiezingen 2019 - Verslag van het College van Deskundigen
Brussel, 7 juni 2019.

Voor het College

Emmanuel Willems
Voorzitter

Bart Martens
Secrétaire