Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Facteurs à considérer en matière de sécurité pour les systèmes de registre électronique du scrutin

SÉRIE GESTIONNAIRES

TLP:WHITE

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, prière d'envoyer un courriel ou de téléphoner au Centre de coordination des services du Centre pour la cybersécurité :

Centre de coordination des services

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 7 février 2022.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	7 février 2022

Aperçu

Le présent document offre des directives sur les facteurs à considérer en matière de cybersécurité pour assurer la conception, le déploiement et le fonctionnement sécurisés des systèmes de registre électronique du scrutin. Le document décrit les fonctions habituelles du registre du scrutin et présente de nouveaux services pouvant être intégrés pour appuyer les élections modernes.

Il donne également des recommandations sur les contrôles de configuration de sécurité que les autorités électorales peuvent prendre en compte lors de l'évaluation, de la conception ou du déploiement de systèmes de registre électronique du scrutin.

ISBN 978-0-660-42357-9
CAT D97-4/10-101-2022F-PDF

Table des matières

Liste des figures

Liste des tableaux

1 Introduction

Les élections modernes sont de plus en plus axées sur des outils de technologies de l'information conçus pour optimiser les processus et accroître la transparence. Plusieurs pays, dont l'Estonie, la Norvège et le Canada, ont mis en œuvre diverses formes de modes de scrutin électronique pour gérer des élections démocratiques. Ces modes ont donné des résultats variables. Le recours à des registres électroniques du scrutin est courant dans le cadre de la plupart des stratégies de modernisation des élections. Ces registres offrent une plateforme multifonction qui favorise une plus grande efficacité et permet d'optimiser les activités le jour du scrutin.

Les registres du scrutin traditionnels sont généralement des documents papier servant principalement aux contrôles manuels des électeurs. Bien que ceux-ci soient considérés comme des documents particulièrement fiables, ils s'avèrent cependant inappropriés pour optimiser efficacement les activités le jour du scrutin. Les registres du scrutin en papier peuvent retarder le traitement des votes et entraîner des erreurs humaines le jour du scrutin. Ils ne sont également pas adaptés pour prendre en charge des services plus récents comme le suivi de la participation en temps réel, pour ainsi permettre une gestion efficace des ressources pour le scrutin. Les technologies liées aux registres électroniques du scrutin peuvent aider à résoudre certains de ces problèmes, et elles peuvent présenter de nouvelles possibilités de services supplémentaires pour améliorer les processus le jour du scrutin.

Le présent document expose certains des avantages que procure l'utilisation de registres électroniques du scrutin, mais il met surtout l'accent sur les facteurs de sécurité à considérer pour protéger son déploiement.

1.1 Architecture, normes et technologies du mode de scrutin électronique

Bien que le Canada ne fasse qu'une utilisation minimale de la technologie pour le processus de vote lors des élections fédérales, plusieurs activités d'arrière-plan dépendent quand même de systèmes technologiques. Par exemple, des activités menées le jour du scrutin comme la communication et le regroupement des résultats du scrutin sont réalisées au moyen de systèmes de technologies de l'information qui utilisent des systèmes de télécommunication et des technologies Web.

On s'attend à ce que les organismes électoraux recensent des occasions d'améliorer les composantes du processus électoral. Le recours à la technologie peut aider à réaliser ces objectifs, mais il peut aussi entraîner des résultats non désirés (p. ex., introduire des vulnérabilités de sécurité dans le processus électoral). Par conséquent, il est important de mettre l'accent sur des pratiques de sécurité sûres pour appliquer une stratégie de transformation électorale moderne. Les sections qui suivent présentent une architecture générale pour les modes de scrutin électronique et abordent la question des registres électroniques du scrutin ainsi que des stratégies visant une gestion sécurisée de ces registres.

1.1.1 Architecture du mode de scrutin électronique

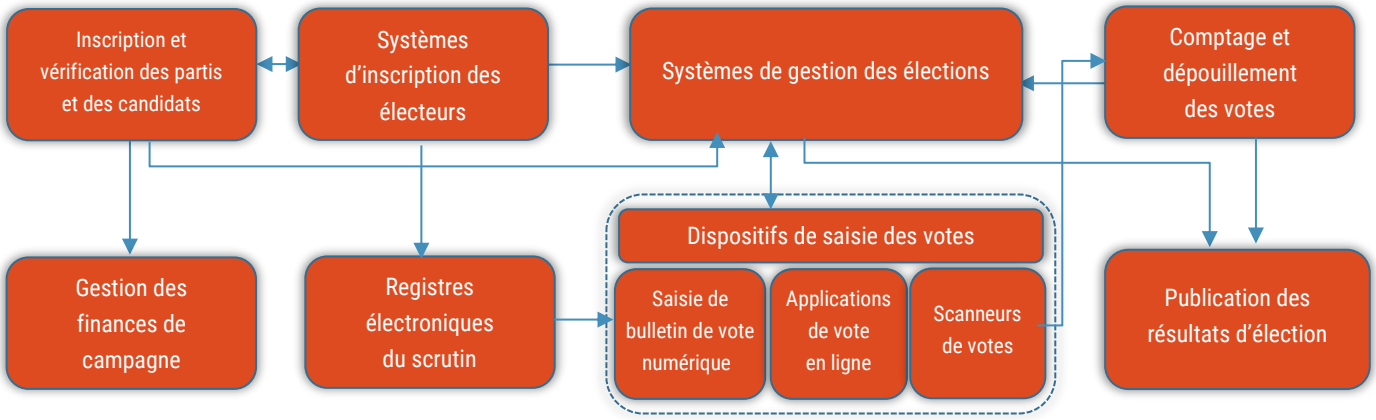
L'architecture du mode de scrutin électronique décrit les composantes des systèmes d'information sollicitées dans le cadre du vote électronique et la manière dont elles interagissent entre elles. Ces systèmes comprennent notamment :

- les sites Web publics;
- les systèmes d'inscription des partis;
- les systèmes d'inscription des électeurs;

- les systèmes de gestion des élections;
- les modes de scrutin par Internet;
- les systèmes de dépouillement des votes;
- les systèmes de publication des résultats.

Ces systèmes, qui exécutent souvent des technologies disparates, sont interconnectés et communiquent entre différents protocoles réseau. Basé sur le guide *A Handbook for Elections Infrastructure Security* publié par le Center for Internet Security (CIS), une architecture générique de modes de scrutin électronique moderne est présentée dans la figure 1. [1]

Figure 1 : Architecture générique de systèmes électoraux



Touche	Description
→	Chemin du flux de données
▭	Composante de système électronique

Étant donné qu'elles touchent précisément les modes de scrutin électronique, une ou plusieurs de ces capacités essentielles peuvent être mises en œuvre au moyen de systèmes informatiques (logiciel et matériel). Certaines de ces composantes peuvent communiquer par Internet ou par des réseaux privés de communication.

2 Registres électroniques du scrutin

Les registres du scrutin, aussi appelés listes électorales, contiennent des renseignements personnels sur les électeurs approuvés dans une zone électorale donnée. Cette liste comporte des renseignements approuvés sur les électeurs auxquels se fie le personnel du bureau de vote. Un registre électronique du scrutin est un appareil électronique qui exécute une application logicielle permettant de gérer la liste des électeurs approuvés dans une région électorale. Le personnel du bureau de vote utilise les données du registre du scrutin pour rechercher et confirmer l'identité des personnes qui se présentent pour voter. Il existe deux principaux modèles pour le déploiement des registres du scrutin : le modèle autonome et le modèle en réseau.

2.1 Modèles de déploiement pour les registres électroniques du scrutin

Les registres électroniques du scrutin peuvent être déployés selon un modèle autonome ou en réseau. Le tableau 1 présente certaines caractéristiques de chacun des modèles de déploiement.

Tableau 1 : Modèle autonome par rapport au modèle en réseau

	Modèle autonome	Modèle en réseau
Description générale	Ce modèle comporte le déploiement et le fonctionnement du registre du scrutin sans connectivité réseau. Avant une élection, les données sur l'inscription des électeurs sont migrées vers les registres du scrutin pour gérer les activités le jour du scrutin.	Ce modèle comporte le déploiement des registres du scrutin au moyen d'une connectivité de réseau partielle ou complète. La communication se fait en général avec un réseau central de gestion des élections sur Internet (public). Les déploiements de registres du scrutin en réseau donnent l'avantage supplémentaire de pouvoir prendre en charge des services en temps réels.
Connectivité Internet et Wi-Fi	Le dispositif du registre du scrutin n'est pas connecté à un réseau Wi-Fi ou à Internet lorsqu'il est dans un environnement de production.	Le dispositif de registre du scrutin peut être connecté ou non à un réseau Wi-Fi ou à Internet pour les activités le jour du scrutin.
Migration des données	La migration des données, y compris celle de l'inscription des électeurs, se fait avant le jour du scrutin. Les données sont transférées par une interface (p. ex., USB ou Wi-Fi). La migration des données est désactivée pour les activités le jour du scrutin.	Ce modèle prend en charge la migration des données hors ligne et en ligne. Les données peuvent être migrées de façon continue sur un réseau ou par un transfert de données programmé le jour du scrutin.
Activités le jour du scrutin	Les déploiements ne peuvent pas faciliter les capacités à « voter n'importe où » pendant une élection.	Certains déploiements peuvent faciliter les capacités à « voter n'importe où », ce qui permet à un électeur de voter à l'extérieur de sa circonscription locale.
Mises à jour logicielles	Lorsque le dispositif de registre du scrutin est déployé, les mises à jour en temps réel des logiciels ou du système ne sont pas offertes.	Ces mises à jour peuvent être prises en charge même après le déploiement pour les activités le jour du scrutin.

2.1.1 Avantages des registres électroniques du scrutin

Les registres électroniques du scrutin procurent notamment les avantages suivants :

- améliorer l'efficacité du processus d'accréditation et de validation;
- réduire ou éviter les erreurs manuelles grâce à l'automatisation du contrôle des électeurs et des rapports;
- rediriger les électeurs au bureau de vote approprié;
- réduire la fraude électorale en repérant facilement les incidents où des électeurs sont associés à plusieurs bulletins de vote;
- soutenir la prestation de services supplémentaires comme l'inscription d'électeurs le jour du scrutin, la validation de l'identité des électeurs et la production de rapports en temps réel.

2.2 Menaces visant les systèmes de registre électronique du scrutin

Il peut s'avérer avantageux de faire appel à la technologie pour appuyer ou remplacer les processus électoraux manuels. Toutefois, des menaces ou des vulnérabilités involontaires peuvent être introduites. Ces menaces peuvent être liées à la manipulation physique du dispositif de registre du scrutin, à la configuration des composantes matérielles, à des défauts dans le code logiciel, à des attaques de la chaîne d'approvisionnement ou à des vulnérabilités associées à l'infrastructure de communication en réseau. L'utilisation d'applications de registre électronique du scrutin durant une élection, que ce soit au moyen d'un modèle autonome ou en réseau, entraînerait fort probablement une augmentation de la surface d'attaque. Ainsi, il est essentiel de déterminer de manière proactive ces menaces et de mettre en œuvre des mesures appropriées pour protéger les systèmes touchés.

Il convient de noter que la liste ci-dessous n'est pas exhaustive. Nous recommandons aux organisations d'effectuer une modélisation des menaces dans le cadre des évaluations des menaces et des risques afin d'identifier et de recenser de façon adéquate les menaces associées aux exigences organisationnelles de déploiement.

1. **Attaques contre l'intégrité des données** : Les systèmes de registre électronique du scrutin renferment des données sensibles, y compris des renseignements sur les électeurs, les processus de vote et les systèmes électoraux. L'altération des données, la destruction accidentelle de données, l'erreur humaine et les attaques par mystification sont des exemples de menaces pouvant entraîner des répercussions sur l'intégrité des données.
2. **Atteintes à la sécurité cryptographique :** Les contrôles cryptographiques, comme le chiffrement, sont utilisés pour protéger la confidentialité et l'intégrité des données inactives et en transit sur les systèmes de registre électronique du scrutin. Des lacunes dans la mise en œuvre de l'algorithme cryptographique peuvent permettre à des auteurs de menace de compromettre les mécanismes de protection cryptographique des données.
   Des vulnérabilités dans le logiciel cryptographique, une mauvaise gestion des clés et des configurations inadéquates représentent des enjeux importants en matière de sécurité qui méritent une attention particulière. L'évolution de la technologie quantique et l'augmentation de la puissance de calcul deviennent également une menace croissante. Les publications *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017)* [2] et *Faire face à la menace que l'informatique quantique fait peser sur la cryptographie (ITSE.00.017)* [3] contiennent plus de détails sur les menaces liées à l'informatique quantique.

3. **Attaques sans fil** : La commodité des réseaux sans fil constitue une solution avantageuse pour les organisations. Les réseaux sans fil peuvent aussi constituer une cible attrayante pour les auteurs de menace. En effet, les réseaux sans fil non sécurisés ouvrent la porte au piratage Wi-Fi, aux attaques de l'intercepteur (PITM pour *Person-in-the-Middle*) et aux attaques par reniflage de trafic réseau. Les réglages par défaut sur des appareils sans fil peuvent également introduire des vulnérabilités pouvant être exploitées. Les réseaux non distincts peuvent accroître l'incidence des dommages aux actifs informatiques lors d'une attaque réussie. Les pirates peuvent alors passer facilement d'un segment de réseau à un autre.
4. **Déni de service distribué (DDoS)** : En l'absence de mécanismes de protection appropriés, l'infrastructure prenant en charge les systèmes de registre électronique du scrutin pourrait être ciblée par des attaques DDoS. Les auteurs de menace peuvent déployer un maliciel pour perturber les opérations et inonder les serveurs, ce qui occasionne des problèmes de disponibilité et d'épuisement des ressources, et entraverait l'accès à l'infrastructure de registre électronique du scrutin. Ces attaques perturbatrices peuvent être utilisées pour réprimer les votes lorsque les attaques visent un segment de l'électorat.
5. **Attaques par maliciel** : Les auteurs de menace peuvent avoir recours à des attaques par hameçonnage et par piratage psychologique, à des attaques de la chaîne d'approvisionnement et à d'autres techniques sophistiquées pour infecter au moyen d'un maliciel les systèmes de registre électronique du scrutin. Ils peuvent utiliser des logiciels malveillants pour permettre l'entrée initiale et faciliter des attaques concertées additionnelles.
6. **Violation de données** : Une erreur humaine ou des attaques lancées par des auteurs de menace peuvent mener à la divulgation de renseignements personnels ou sensibles. Des interventions involontaires de la part de parties prenantes aux élections peuvent entraîner une atteinte à la protection des données, ce qui pourrait compromettre la confidentialité et l'intégrité d'un système de registre électronique du scrutin. Des personnes non autorisées pourraient avoir accès à des renseignements confidentiels comme des clés cryptographiques, des données relatives aux bulletins de vote, des mots de passe et des renseignements sur les électeurs.
7. **Vulnérabilités système** : Les vulnérabilités (logicielles ou matérielles) présentes dans les composantes de l'infrastructure pourraient être utilisées pour manipuler ou mettre à jour les renseignements sur les électeurs. Les vulnérabilités système peuvent être exploitées dans le but de compromettre l'intégrité du système de registre du scrutin. Chaque composante de l'infrastructure du scrutin électronique pourrait être vulnérable.

3 Facteurs de sécurité à considérer pour les registres électroniques du scrutin

La sécurité de l'infrastructure de registre électronique du scrutin de votre organisation repose principalement sur l'efficacité des contrôles mis en place pour sécuriser votre matériel, vos logiciels, votre réseau et vos données. Les contrôles de sécurité déployés doivent travailler conjointement et se compléter pour être en mesure d'éliminer les lacunes et les menaces associées à votre déploiement.

Les registres électroniques du scrutin doivent être déployés sous forme de système à usage unique.

Les recommandations mentionnées ci-dessous sont des facteurs à considérer afin de réduire au minimum les risques liés à l'utilisation de systèmes de registre électronique du scrutin lors des élections. Ces recommandations ne constituent pas une liste exhaustive de considérations en matière de sécurité. Votre organisation devrait envisager d'effectuer une évaluation des menaces et des risques pour s'assurer que les mesures de sécurité mises en œuvre sont adaptées aux menaces associées à votre infrastructure de registre électronique du scrutin.

1. **Établir un cadre directeur et un ensemble de principes pour l'utilisation de technologies numériques.** La mise en œuvre d'un cadre directeur offrant une protection juridique adéquate en ce qui a trait à l'utilisation de technologies numériques dans le processus électoral représente une étape de base importante. La mise en place d'un mandat législatif et de principes directeurs pertinents permettra d'assurer que les nouveaux systèmes numériques respectent les processus électoraux existants, et d'assurer la préservation des valeurs démocratiques de base. Des valeurs telles que l'anonymat de l'électeur, la justice, l'intégrité et la transparence représentent des piliers fondamentaux sur lesquels votre stratégie électorale numérique, y compris l'utilisation de registres électroniques du scrutin, devrait reposer. Un cadre directeur pour des élections numériques peut également s'avérer utile afin d'évaluer le caractère adéquat des solutions électroniques et des services tiers proposés.
2. **Choisir des solutions conçues au moyen de normes de pratiques exemples en matière de sécurité.** Les normes de sécurité prises en charge par tout registre du scrutin devraient vraisemblablement influencer le choix des contrôles offerts en vue d'un déploiement. Il faut s'assurer que le registre électronique du scrutin choisi est conforme aux normes en matière de pratiques exemplaires et de développement sécurisé. Les solutions de registre du scrutin développées en fonction de pratiques exemplaires en matière de programmation sécurisée favoriseront la sécurité, la fiabilité et la résilience de l'ensemble du système. La conformité à des normes de développement d'applications comme les directives sur la programmation sécurisée de la communauté Open Web Application Security Project (OWASP), les contrôles de sécurité essentiels du Center for Internet Security (CIS) et les pratiques de code sécurisé de l'organisation MITRE permet d'éviter des pratiques de développement logiciel dangereuses. Les solutions intégrant des normes en matière de pratiques exemplaires procurent des avantages sur les plans de l'interopérabilité, la résilience et la sécurité. Il faut également tenir compte d'autres normes pour assurer une harmonisation, notamment les normes de la Federal Information Processing Standards (FIPS) et celles de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI).

3. **Sélectionner des produits provenant de chaînes d'approvisionnement vérifiables et traçables.** Il est essentiel de veiller à ce que les produits et les solutions qui soutiennent les processus démocratiques soient associés à des chaînes d'approvisionnement pouvant être vérifiées et retracées. Certains auteurs étatiques exploitent l'accès aux chaînes d'approvisionnement mondiales pour compromettre des systèmes en développement. La direction devrait instaurer un programme de gestion des risques liés à la chaîne d'approvisionnement (GRCA) pour assurer la surveillance et l'intégration des processus d'achat. L'organisation devrait intégrer les exigences en matière de GRCA à ses processus et effectuer des évaluations périodiques de même que des vérifications approfondies préalables auprès des fournisseurs pour évaluer les modifications apportées à leur structure de propriété ou à leurs relations. Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) offre des services d'évaluation des risques liés à la chaîne d'approvisionnement pour appuyer les secteurs des infrastructures essentielles du Canada, ce qui comprend les institutions démocratiques. Les organes de gestion électorale peuvent obtenir de l'aide pour évaluer les composantes essentielles de leur infrastructure d'élection numérique. La publication du Centre canadien pour la cybersécurité intitulée *Menaces à la chaîne d'approvisionnement et espionnage industriel* [4] contient de plus amples renseignements.
4. **Mettre en œuvre des mécanismes de protection cryptographique et des contrôles de sécurité de bout en bout.** La sécurité de toutes les données sensibles, comme les dossiers électroniques des électeurs, doit être un objectif prioritaire de chaque registre électronique du scrutin. Des contrôles de chiffrement et d'intégrité des données pour protéger les données du registre électronique du scrutin sont fortement recommandés. De plus, afin de remédier aux risques liés à la confidentialité et à l'intégrité des données, les données inactives ou en transit sur le support du registre électronique du scrutin doivent être chiffrées. Les mécanismes de protection cryptographique offerts dans les systèmes d'exploitation modernes pour protéger les données en mémoire devraient être activés. Le chiffrement des données doit être réalisé uniquement au moyen d'applications dotées d'algorithmes approuvés par les normes FIPS 140-2/140-3. La page Web sur le Programme de validation des modules cryptographiques (PVMC) [5] du Centre pour la cybersécurité renferme les plus récentes lignes directrices sur les normes cryptographiques approuvées. Les mots de passes et clés de session et de chiffrement doivent être gérés adéquatement de manière à éviter toute compromission. Que l'application de registre du scrutin soit exécutée sur le nuage ou hors nuage, l'organisation pourrait aussi opter pour d'autres contrôles de sécurité des données avancés comme le masquage de données, la classification des données et des techniques de segmentation en unités pour protéger des champs et des valeurs précis de données sensibles. La segmentation en unités est un processus automatisé de remplacement d'éléments de données sensibles par des données non sensibles. De plus amples renseignements sur les techniques de segmentation en unités sont fournis dans les publications du Centre pour la cybersécurité intitulées *Guide sur le chiffrement des services infonuagiques (ITSP.50.106)* [6] et *Guide sur la segmentation en unités dans le cadre des services fondés sur l'infonuagique (ITSP.50.108)* [7].
5. **Mettre en œuvre des contrôles de sécurité réseau pour sécuriser les communications.** Ne connectez les dispositifs de registre électronique du scrutin qu'à des réseaux sans fil ou câblés approuvés. Mettez en œuvre des contrôles de séparation et de segmentation réseau pour le réseau de registre du scrutin. Mettez en place la technologie du routage et du réacheminement virtuels (VRF pour *Virtual Routing and Forwarding*) pour segmenter de manière logique le trafic de la couche 3, des réseaux locaux virtuels (VLAN pour *Virtual Local Area Network*) pour le trafic de la couche réseau 2 et des coupe-feux sur hôte pour limiter et gérer le trafic vers et depuis le réseau de registre du scrutin. Veillez à ce que les contrôles de filtrage d'application soient installés de façon à empêcher que

des demandes malveillantes ne compromettent les dispositifs de registre du scrutin. Utilisez des réseaux privés virtuels (RPV) pour sécuriser les communications provenant du registre du scrutin allant vers d'autres dispositifs sur le réseau. Choisissez des solutions de chiffrement de RPV en fonction uniquement d'algorithmes approuvés et évitez d'utiliser des protocoles désuets. Pour en apprendre davantage sur les RPV, veuillez consulter la publication *Les réseaux privés virtuels* (ITSAP.80.101) [8] du Centre pour la cybersécurité. Par ailleurs, envisagez la mise en œuvre de mécanismes d'authentification mutuelle pour vous assurer que tous les dispositifs sont authentifiés. Les principes de sécurité à vérification systématique doivent être pris en compte lors de la conception et de l'intégration des composantes de votre réseau de registre du scrutin. Évitez d'avoir une confiance implicite dans les composantes réseau. Authentifiez et autorisez continuellement les actifs et services réseau. Limitez l'accès physique aux points d'accès réseau pour assurer une protection contre les attaques physiques.

6. **Mettre en œuvre des politiques d'authentification multifacteur et de mots de passe robustes.** Afin d'atténuer le risque d'accès non autorisés et d'attaques de mot de passe, mettez en œuvre l'authentification multifacteur sur vos dispositifs et votre application de registre du scrutin. Établissez et appliquez des politiques de mots de passe sécurisés comme l'utilisation de mots de passe robustes et l'interdiction de partager des comptes sur les dispositifs. Changez les noms d'utilisateur et les mots de passe par défaut sur le dispositif et l'application du registre du scrutin avant le déploiement sur le terrain. Dans des scénarios où l'authentification par biométrie est mise en œuvre, les contrôles de détection du vivant doivent être pris en charge. Les techniques de détection du vivant permettent de détecter si un ensemble de données biométriques présenté provient d'une personne réelle ou d'une tentative d'usurpation d'identité (image, photo, vidéo ou enregistrement sonore). Mettez en place des mesures de blocage de compte ou des capacités d'effacement à distance sur les dispositifs pour protéger les données après plusieurs échecs d'authentification. Pour obtenir de plus amples renseignements sur la sécurité relative à l'authentification, aux mots de passe et à la biométrie, consultez les publications suivantes du Centre pour la cybersécurité : *Biométrie (ITSAP.00.019)* [9], *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032*) [10] et *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)* [11].

7. **Limiter les droits d'accès aux personnes qui en ont besoin pour remplir leurs tâches.** Mettez en place des mécanismes de contrôle d'accès. Les permissions d'accès accordées au personnel des bureaux de scrutin doivent correspondre aux tâches prévues. Évitez l'octroi de droits d'utilisation excessifs. Adoptez des principes de sécurité comme celui du droit d'accès minimal par défaut et évitez d'utiliser des comptes administratifs pour des tâches non administratives. Enlevez les privilèges d'accès aux systèmes de registre du scrutin dès que les utilisateurs n'en ont plus besoin. De plus amples renseignements sur la protection des comptes se trouvent dans la publication *Gestion et contrôle des privilèges administratifs (ITSAP.10.094)* [12]. Il pourrait aussi s'avérer utile de recourir à des écrans qui se verrouillent après une période d'inactivité ou à des contrôles de blocage de compte.

8. **Désactiver les services ou interfaces de communication de données non utilisés.** Les interfaces de communication sur les dispositifs de registre du scrutin, comme les interfaces réseau, les interfaces USB et la technologie Bluetooth, qui ne sont pas utilisées pour le transfert de données, doivent être désactivées. Mettez en œuvre des contrôles de renforcement système pour vous assurer que les services système non utilisés sont bloqués. Renforcez les dispositifs de registre du scrutin et de communication réseau en désactivant les services non protégés et les protocoles faibles comme Telnet et SSL version 3.0. Adoptez des procédures qui permettent de

déployer les composantes du système de registre électronique du scrutin à l'aide de processus normalisés et de paramètres de configuration sécurisés. Mettez en œuvre des contrôles de changement de configuration qui permettent de limiter ou d'empêcher les modifications non approuvées au système.

9. **Configurez des systèmes de registre du scrutin sous forme de systèmes à usage unique.** Lorsque cela est possible, il est recommandé que les registres électroniques du scrutin soient configurés sous forme de système à usage unique afin de réduire la surface d'attaque probable. D'autres fonctions système comme la navigation Web et les services de courriel ne devraient pas être autorisées sur les dispositifs. Appliquez des contrôles de sécurité pour verrouiller les dispositifs de registre du scrutin afin que seules les tâches du registre du scrutin ou les tâches approuvées puissent être exécutées sur le dispositif. Envisagez l'intégration de mécanismes de contrôle pouvant déclencher des alarmes si le registre du scrutin s'écarte de sa fonctionnalité souhaitée.
10. **Effectuer une évaluation périodique des menaces et des risques pour les systèmes de registre électronique du scrutin.** Il est essentiel de vérifier régulièrement la sécurité du système, plus particulièrement avant son déploiement en vue d'une élection. Effectuez une évaluation des menaces et des risques pour identifier et comprendre les risques associés aux technologies électorales déployées. Une telle évaluation du système de registre du scrutin permettra de concentrer les efforts sur la prévention des risques clés. Recueillez des renseignements sur les menaces pour avoir une meilleure connaissance de la situation et vous tenir informé des menaces actuelles. Dans la mesure du possible, les essais et les évaluations doivent être effectués le plus près possible des configurations de production, par exemple sur des dispositifs fonctionnant avec une connectivité Wi-Fi, un accès Internet et une connectivité avec d'autres applications. L'application de scénarios de test pour les systèmes en réseau ou autonomes devrait également refléter le déploiement de production de ces systèmes.
11. **S'assurer que les plans d'urgence opérationnels comprennent des sauvegardes du système, des sauvegardes papier et des options d'alimentation électrique de secours.** Veillez à ce que les dispositifs de registre du scrutin soient pleinement chargés avant le déploiement aux bureaux de vote le jour du scrutin. Les dispositifs doivent être branchés dans des prises électriques adéquates. Assurez-vous que vos plans de reprise et de continuité des activités offrent des mesures pour gérer les situations d'urgence en cas de pannes d'électricité. Si les dispositifs peuvent fonctionner en mode économie d'énergie, confirmez que les applications et le déploiement ont été entièrement testés dans le cadre d'exercices d'urgence. Mettez en œuvre une solution de sauvegarde du système pour stocker et récupérer les données du système. Assurez-vous que les sauvegardes de données sont stockées hors ligne et débranchées du réseau, des dispositifs et des systèmes de l'organisation afin d'éviter la propagation de rançongiciels et d'autres maliciels. Testez vos sauvegardes dans le cadre de vos activités de planification d'urgence. Il est possible que le registre électronique soit inaccessible ou inutilisable pendant l'élection, il est donc important d'inclure un système de sauvegarde papier à votre procédure de reprise en cas d'incident. Le personnel du bureau de vote doit recevoir une formation adéquate sur la mise en fonction des registres du scrutin papier, plus particulièrement durant un événement électoral. Bien que l'exécution d'un système de registre du scrutin en mode hors ligne puisse être considérée comme une option de reprise de service (p. ex., pour les systèmes en ligne), les sauvegardes papier devraient toujours faire partie des plans d'urgence.
12. **Maintenir un contrôle strict des dispositifs de registre du scrutin et conserver la chaîne de possession des documents.** Il est important de bien gérer les déplacements et les emplacements des dispositifs de registre du scrutin. Des procédures adéquates doivent être mises en œuvre pour suivre physiquement les dispositifs de registre du scrutin et les protéger, notamment l'application de contrôles de stockage physique, d'accusés de réception écrits

et de processus de soutien. Les dispositifs de registre du scrutin comportant des données (chiffrées ou non) ne devraient pas franchir les frontières internationales étant donné que leur contenu pourrait être assujetti à différentes législations. Les membres du personnel et le personnel des bureaux de scrutin doivent recevoir une formation adéquate sur la façon de se conformer aux procédures de la chaîne de possession. Les capacités d'effacement à distance sur les dispositifs doivent être accessibles en cas de vol de dispositif.

13. **Mettre en œuvre des mécanismes de protection et de défense contre le code malveillant.** Un registre électronique du scrutin connecté à Internet augmente les risques de code malveillant ou de maliciels. L'installation d'antimaliciels et d'antivirus est nécessaire pour détecter la présence d'un logiciel malveillant sur un dispositif et le neutraliser. Afin d'empêcher l'exécution d'un code malveillant, envisagez le recours à des contrôles de renforcement système comme la mise en place de restrictions liées à l'exécution des applications, le blocage de l'exécution de scripts non autorisés et le verrouillage des comptes administratifs pour empêcher leur accès à Internet. Les mises à jour logicielles doivent être installées rapidement et les composants logiciels obsolètes doivent être supprimés.

14. **Assurer le maintien d'une configuration de base sécurisée.** Pour assurer la cohérence et la conformité législative, votre organisation doit élaborer et consigner un ensemble d'exigences de sécurité obligatoires pour développer, déployer et faire fonctionner les registres électroniques du scrutin. Dans certains cas, il peut s'avérer nécessaire d'élaborer un ensemble renforcé d'exigences afin de prévenir des scénarios de menaces précis ou de répondre à des besoins opérationnels pour des cas d'utilisation précis. Ces bases de référence doivent être mises à jour régulièrement au besoin, plus particulièrement lorsque des vulnérabilités ayant une incidence sur ses composants de base sont détectées. Testez et recertifiez les bases de référence lorsque des modifications sont apportées ou que de nouvelles mises à jour sont appliquées.

15. **Mettre en œuvre des procédures sécurisées de nettoyage des dispositifs pour les registres du scrutin mis hors service.** Dans le cadre du processus de mise hors service ou d'élimination, les supports électroniques sur les dispositifs de registre du scrutin doivent être nettoyés correctement. Il faut choisir des procédures de nettoyage de données appropriées en fonction du format du support électronique. À titre d'exemple, la démagnétisation peut convenir à des lecteurs magnétiques, mais pas au stockage de supports utilisant des disques électroniques. Il est important d'adapter vos processus de mise hors service aux composants concernés. Pour obtenir de plus amples renseignements, consultez la publication du Centre pour la cybersécurité intitulée *Nettoyage et élimination d'appareils électroniques (ITSAP.40.006)* [13].

16. **Authentifier et valider continuellement les dispositifs de registre du scrutin.** Surveillez régulièrement l'état des dispositifs et les activités des systèmes, et déclenchez les mesures nécessaires lorsque l'état change. Mettez en œuvre des politiques de sécurité pour identifier les risques de façon permanente. Les changements apportés aux micrologiciels, au processus de démarrage et au système d'exploitation sont certains paramètres importants à surveiller pour vérifier la conformité et protéger l'état de la configuration. Les résultats tirés d'une analyse d'antivirus et d'autres vérifications heuristiques de comportement sont des paramètres pouvant également faire l'objet d'un suivi. Assurez-vous que les dispositifs de registre du scrutin répondent aux critères prévus en matière d'état sécurisé avant d'obtenir l'accès au réseau central de gestion des élections.

17. **Activer les contrôles d'isolation d'applications et de bac à sable.** Pour protéger l'application du registre du scrutin et limiter les interactions avec ses données et ressources, il est possible de mettre en œuvre des mécanismes d'isolation d'applications et de bac à sable. Les contrôles d'isolation d'applications permettent de limiter les

opérations non autorisées sur l'application de registre du scrutin et ses données. La majorité des systèmes d'exploitation modernes prennent en charge l'exécution d'applications dans des environnements conteneurisés ou de type bac à sable. De plus, l'exécution d'applications de logiciel tiers au sein d'un environnement bac à sable sur le dispositif de registre du scrutin contribuera à limiter ses répercussions sur d'autres parties du système de registre du scrutin en cas de compromission. Des techniques comme l'utilisation de signatures de code numérique et de politiques de contrôle d'application d'exécution sont des mesures supplémentaires à envisager pour protéger l'intégrité du système et empêcher l'exécution de code non fiable.

18. **Mettre à jour le logiciel de façon ponctuelle et supprimer les applications obsolètes.** Les applications obsolètes ou non maintenues peuvent exposer les systèmes de registre du scrutin à plusieurs vulnérabilités. Assurez-vous qu'il y ait un suivi des mises à jour permettant de corriger les vulnérabilités et que les correctifs logiciels soient testés et appliqués rapidement. Pour en savoir plus, consultez le document *Application des mises à jour sur les dispositifs (ITSAP.10.096)* [14]. Il faut prévoir des mises à jour logicielles pour les dispositifs de registre du scrutin qui n'ont aucune connexion réseau directe, ainsi que pour les logiciels et le matériel liés aux systèmes de scrutin. Il faut prévoir suffisamment de temps pour installer complètement toutes les mises à jour requises avant que les dispositifs soient déployés pour une élection.

19. **Autoriser la journalisation et la surveillance des activités système.** Il faut activer la journalisation au niveau du système d'application et les journaux d'activités réseau. Lorsque cela est possible, la stratégie de journalisation et de surveillance devrait comprendre la collecte des journaux en temps réel afin d'assurer leur intégrité.

20. **Mettre en œuvre des politiques et des procédures pour gérer les atteintes à la vie privée.** Mettez en œuvre des politiques et des procédures pour protéger les renseignements personnels conservés sur les dispositifs de registre électronique du scrutin. Mettez en place des procédures pour enquêter sur les incidents relatifs aux atteintes à la vie privée, y intervenir et produire des rapports connexes. Assurez-vous d'obtenir le consentement pour la collecte, l'utilisation et la divulgation des renseignements sur les utilisateurs. Avisez les utilisateurs touchés par les atteintes qui ont des répercussions sur leurs renseignements personnels.

4 Conclusion

Les registres électroniques du scrutin peuvent être très utiles pour la gestion et l'amélioration des activités le jour du scrutin, mais s'ils ne sont pas déployés de façon sécurisée, ils peuvent présenter des risques additionnels pour le processus électoral. Entre autres avantages, ils créent des occasions très intéressantes d'offrir une prestation efficace des processus de contrôle des électeurs. En raison de leur capacité à détenir de grandes quantités de données et de renseignements sensibles sur les électeurs, les registres électroniques du scrutin représentent des cibles intéressantes pour les auteurs de menace. Il est nécessaire d'adapter les contrôles de sécurité mis en place aux besoins particuliers de chaque organe de gestion électorale.

Les solutions de sécurité choisies devraient être orientées vers la préservation de l'objectif de confidentialité, d'intégrité et de disponibilité du processus électoral. Les pratiques exemplaires et les technologies modernes devraient être au cœur de la conception, du développement et de l'exploitation de ces systèmes. Chaque compétence doit être en mesure d'évaluer ses scénarios de déploiement et de mettre en œuvre des contrôles adéquats pour protéger son système. Il est important de savoir que les registres du scrutin ne représentent qu'une composante de l'architecture du vote électronique. La sécurité de leur déploiement dépend en partie de l'intégration sécurisée dans le reste de l'écosystème des élections numériques.

5 Contenu complémentaire

5.1 Liste des acronymes, abréviations et sigles

Terme	Définition
CST	Centre de la sécurité des télécommunications
GC	Gouvernement du Canada
STI	Sécurité des technologies de l'information
TI	Technologies de l'information

5.2 Glossaire

Terme	Définition
Atteinte à la vie privée	Collecte, consultation, utilisation, conservation, divulgation ou élimination inappropriée de renseignements personnels ayant une incidence sur la vie privée de la personne à qui appartiennent ces renseignements.
Électeur	Tout citoyen canadien âgé d'au moins 18 ans.
Évaluation des menaces et des risques	Processus qui permet d'établir les actifs du système et la façon dont ils peuvent être compromis, d'évaluer le niveau de risque que posent les menaces pour les actifs et de recommander des mesures de sécurité pour atténuer les menaces.
Information sensible	Information susceptible de causer des dommages, de l'embarras ou des désagréments à une personne ou à une entité en cas de perte, de compromission ou de divulgation.
Registre du scrutin	Liste d'électeurs approuvés pour une zone électorale particulière.
Réseau privé virtuel (RPV)	Réseau de communication privé généralement utilisé au sein d'une organisation ou par plusieurs entreprises ou organisations diverses pour communiquer sur un réseau élargi. Les communications sur le RPV sont habituellement chiffrées ou codées pour protéger le trafic provenant des autres utilisateurs, qui est transmis sur le réseau public ayant recours au RPV.
Routage et réacheminement virtuels (VRF pour *Virtual Routing and Forwarding*)	Technologie qui permet à plusieurs instances d'une table de routage de coexister au sein du même routeur en même temps.
Segmentation en unités	Processus qui consiste à remplacer certains éléments des données sensibles par des équivalents non sensibles, appelés jetons, qui n'ont aucune signification ou valeur extrinsèque ou exploitable.

5.3 Références

Numéro	Référence
1	Center For Internet Security. *A Handbook for Elections Infrastructure Security*, février 2018.
2	Centre canadien pour la cybersécurité. *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017)*, février 2021.
3	Centre canadien pour la cybersécurité. *Faire face à la menace que l'informatique quantique fait peser sur la cryptographie (ITSE.00.017), mai 2020.*
4	Centre canadien pour la cybersécurité. *Menaces à la chaîne d'approvisionnement et espionnage industriel*, décembre 2018.
5	Centre canadien pour la cybersécurité. *Programme de validation des modules cryptographiques (PVMC)*.
6	Centre canadien pour la cybersécurité. *Guide sur le chiffrement des services infonuagiques (ITSP.50.106)*, mai 2020.
7	Centre canadien pour la cybersécurité. *Guide sur la segmentation en unités dans le cadre des services fondés sur l'infonuagique (ITSP.50.108)*, octobre 2021.
8	Centre canadien pour la cybersécurité. *Les réseaux privés virtuels (ITSAP.80.101)*, octobre 2019.
9	Centre canadien pour la cybersécurité. *Biométrie (ITSAP.00.019)*, février 2020.
10	Centre canadien pour la cybersécurité. *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*, septembre 2019.
11	Centre canadien pour la cybersécurité. *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*, juin 2020.
12	Centre canadien pour la cybersécurité. *Gestion et contrôle des privilèges administratifs (ITSAP.10.094)*, juillet 2020.
13	Centre canadien pour la cybersécurité. *Nettoyage et élimination d'appareils électroniques (ITSAP.40.006)*, octobre 2020.
14	Centre canadien pour la cybersécurité. *Application des mises à jour sur les dispositifs (ITSAP.10.096)*, mars 2021.