Budget 2022 : Soutien pour les départements et les agences du gouvernement fédéral canadien pour la cybersécurité et la lutte contre la désinformation

Recherche verticale approfondie pour pouvoir explorer les aperçus adaptés au sein de votre secteur

10 juin 2022

La transformation numérique s'est accélérée depuis le commencement de la pandémie au début 2020 pour servir les attentes changeantes des Canadiens. Les services ont changé pour inclure davantage d'interactions sans contact, que ces services soient dirigés vers l'extérieur pour les électeurs canadiens ou de nature interne.

En parallèle d'une numérisation et d'une dépendance plus importantes imposées sur ces systèmes numériques, les attaques en ligne ont augmenté de manière significative. C'est une grande affaire : D'après un compte publié, le cybercrime est dans les environs de 10,5 billions de dollars américains d'ici 2025. Au Canada, le décompte est estimé à un montant dépassant 3 milliards de dollars canadiens par an. En plus de cet environnement déjà compliqué s'ajoute la montée de la désinformation, informations incorrectes ou trompeuses, dans la sphère numérique.

Cependant, les attaques en ligne ne visent pas seulement l'argent. Des escrocs, la plupart d'entre eux étrangers, s'attaquent aussi aux secrets d'intérêt national et à la propriété intellectuelle, tels que des améliorations en intelligence artificielle ou en informatique quantique, tout ce qui peut apporter un avantage ou égaliser les chances dans l'environnement économique mondial très compétitif de « vainqueur prend tout » d'aujourd'hui.

La protection des systèmes et des réseaux informatiques contre la divulgation et le vol d'informations ou contre les dégâts sur leurs appareils, logiciels ou données électroniques, ainsi que la protection contre la perturbation ou le détournement des services qu'ils fournissent est la mission de la cybersécurité. Mais cet effort devient de plus en plus complexe, un jeu perdu d'avance pour de plus en plus de Canadiens. Par conséquent, le gouvernement canadien a attribué une dépense significative pour les mesures de cybersécurité dans le budget de 2022. Le gouvernement a décrit 875,2 millions de dollars canadiens pour les cinq prochaines années, commençant en FY2022-23, ainsi que 238,2$ millions en cours pour des mesures supplémentaires afin de faire face au « paysage de menace cyber à évolution

rapide ». Des détails supplémentaires étaient également décrits dans le budget (toutes les valeurs sont en dollars canadiens) :

- 263,9 millions sur cinq ans, commençant en 2022-23 et 96,5 millions en cours pour améliorer les capacités du CST [Centre de la sécurité des télécommunications] pour lancer des opérations cyber afin d'empêcher et de se défendre contre les attaques cyber;
- 180,3 millions sur cinq ans, commençant en 2022-23 et 40,6 millions en cours pour améliorer les capacités du CST pour empêcher et répondre aux attaques cyber sur les infrastructures essentielles;
- 178,7 millions sur cinq ans, commençant en 2022-23, et 39,5 millions en cours pour étendre la protection de cybersécurité pour les petits départements, les agences et les corporations de la Couronne; et
- 252,3 millions sur cinq ans, commençant en 2022-23 et 61,7 millions en cours pour le CST pour rendre les systèmes gouvernementaux essentiels plus résilients face aux incidents cyber.

D'autre part, le budget de 2022 a proposé 17,8 millions sur cinq ans, commençant en FY22-23 et 5,5 millions par la suite jusqu'en 2031-32 pour le Centre de la sécurité des télécommunications pour un programme unique de chaires de recherche finançant la recherche sur des technologies de pointe en rapport avec les activités du CST.

Qu'est-ce que cela signifie? Le gouvernement canadien adopte non seulement une vision de plus en plus sophistiquée de la cybersécurité mais adopte également des mesures offensives et défensives dans la poursuite de ses objectifs. La dépense des financements permet au gouvernement de s'étendre sur le plan d'action de cybersécurité nationale décrit initialement dans le budget fédéral de 2018 (ce plan d'action avait été créé à partir d'une analyse cyber complète en 2016 avec des consultations publiques et des avis provenant de secteurs privés et publics).

Bien entendu, le Secrétariat du Conseil du Trésor décrit la direction que les départements doivent suivre, comme décrite dans la politique sur la sécurité gouvernementale et autres directives correspondantes. En effet, les réseaux et la sécurité sont cités comme la priorité numéro un dans Les services partagés du Canada 3.0 : Une approche d'entreprise. Cependant, les enjeux sont plus importants que jamais et la région de la capitale nationale se retrouve à devoir résoudre elle-même des initiatives TI conflictuelles ainsi qu'à devoir entrer en compétition avec le secteur privé dans la guerre pour les talents. Cet environnement très complexe est la base du raisonnement du gouvernement pour continuer à investir dans les mesures de cybersécurité.

Faire la course pour suivre le mouvement

Le rapport sur les priorités de sécurité d'Info-Tech en 2022 couvre cinq priorités de sécurité pour 2022 : acquérir et retenir les talents, sécuriser les employés travaillant à distance, sécuriser la transformation numérique, adopter le Zero Trust et se protéger contre et répondre aux logiciels de rançon. Les

organisations TI font la course pour suivre le mouvement avec le changement. La recherche d'Info-Tech décrit plusieurs recommandations reflétant un monde TI altéré pour toujours par les catalyseurs comme la pandémie mondiale, le travail à distance et le cybercrime devenant de plus en plus sophistiqué. Il est plus important que jamais que les organisations (publiques ou privées) participent aux étapes nécessaires visant à assurer une transformation numérique continuelle. Le coût moyen d'une violation des données était de 4,24 millions de dollars américains en 2021; le coût moyen de violations des données est 1,07 millions de dollars américains plus élevé lorsque le travail à distance est impliqué que lorsqu'il ne l'est pas. Notre ensemble récent de solutions de recherche Priorités de sécurité pour 2022 examine cet environnement changeant en plus de détails et décrit les recommandations pour les départements et les agences du gouvernement du Canada.

Terrain en mouvement constant

Le plan des priorités de cybersécurité en périodes de pandémie par Info-Tech couvre cinq priorités : culture et sensibilisation, sécurité de réseau, sécurité du point final, gestion de la vulnérabilité et gestion des incidents de sécurité.

Depuis que la pandémie mondiale a pris racine, les organisations ont lutté pour trouver le bon équilibre entre la mise en place de contrôles de sécurité trop nombreux, ayant un impact potentiel sur le rendement, et pas suffisamment de sécurité pour assurer que les organisations restent protégées et sures.

Il est essentiel que les départements et les agences de gouvernement couvrent tous les domaines applicables de sécurité TI tout en restant conformes aux directives liées à la sécurité. Une formation en cours et continuelle des utilisateurs finaux, la sécurisation des points finaux et la mise à jour des procédures opérationnelles de réponse de sécurité sont le strict minimum.

Tout commence par une stratégie

Le modèle de stratégie de sécurité d'Info-Tech met l'accent sur la création d'une stratégie qui est alignée sur l'entreprise, consciente des risques et holistique. Il couvre le contexte d'entreprise, les pressions, l'état de la cible de la sécurité, l'état actuel de la sécurité et une feuille de route.

Toutes les institutions, publiques ou privées, doivent avoir une stratégie de sécurité TI qui décrit la direction de la sécurité pour l'organisation et la façon dont la stratégie de sécurité IT doit être atteinte. Il ne peut pas y avoir de substitutions pour les éléments fondamentaux : Une stratégie de cybersécurité aux bonnes dimensions est fondée sur une stratégie de sécurité TI globale de l'organisation. Info-Tech fournit un plan de stratégie de sécurité des informations qui s'aligne avec les objectifs de l'organisation, évalue les risques de l'organisation, incorpore une évaluation complète de l'état actuel et organise la priorité des initiatives de sécurité TI en un plan de sécurité TI. De plus petits départements bénéficient

particulièrement d’une stratégie qui prend en compte leurs environnements plus simples tout en protégeant et en défendant l’organisation contre des escrocs et des attaques cyber; consulter notre manuel spécialisé Construire une stratégie de sécurité d’information pour les petites entreprises.

La cybersécurité dans le contexte du gouvernement fédéral

La diapositive titre du rapport de cybersécurité du gouvernement fédéral, une tendance clé de l’industrie.

Les agences du gouvernement fédéral présentent des caractéristiques uniques, des conditions qui sont devenues encore plus pressantes depuis début 2020. Notre rapport de cybersécurité du gouvernement fédéral décrit ces scénarios en de plus amples détails, offrant un cadre pour aider les départements et les agences à soutenir la stratégie de cybersécurité nationale et pour assurer la confiance continue du public dans les institutions gouvernementales.

Que faire du patrimoine

De nombreux éléments sont couverts par le parapluie de stratégie numérique : principes numériques, objectifs organisationnels, le modèle numérique opératoire et le modèle de distribution numérique travaillent tous ensemble avec leurs nombreux éléments. La plupart des ministères et des départements du gouvernement fédéral du Canada ne sont pas de nouvelles entités. De nombreux départements du gouvernement du Canada sont plus anciens que de nombreuses organisations du secteur privé et en tant que tels, sont plus à même d'être chargés de solutions pour le patrimoine et de processus de maintenance du patrimoine. Les solutions pour le patrimoine pourraient ne pas accommoder les caractéristiques actuelles de sécurité, telles que l'authentification multifactorielle, authentification unique ou RBAC [contrôles d'accès en fonction du rôle], sans compter les nouvelles méthodes de codage. Il est plus difficile pour les solutions pour le patrimoine d’accommoder les modifications avec la flexibilité requise par l’environnement professionnel, ajoutant une pression supplémentaire sur la TI pour rester à jour avec les engagements en matière de gestion des diffusions et des déploiements toujours changeants. De plus, les applications pour le patrimoine souffrent régulièrement de problèmes de conformité, d’absence de soutien par le vendeur et les pénuries de ressources qualifiées. Ce ne sont pas de bons ingrédients pour une transformation numérique.

Bien sûr, les départements le savaient depuis des années, la dernière incarnation d’efforts généralement comprise dans le terme modernisation, un effort impliquant que des équipes TI et commerciales travaillent ensemble pour distribuer des produits et des services de préférence par le biais de la technologie; consulter notre manuel Moderniser vos applications. Dans l’environnement à somme nulle de cybersécurité où une position de sécurité de l’organisation est libellée par son maillon le plus faible, il est essentiel que les départements TI aient un plan en place pour mettre fin à, fortifier ou isoler ces systèmes du patrimoine.

Notre point de vue

Le gouvernement fédéral a réalisé l'importance de la cybersécurité comme un principe clé de la transformation numérique durable. En engageant des financements en cours pour améliorer la disposition de la cybersécurité, il reconnaît la complexité de l'environnement mondial changeant auquel le Canada fait face et investit des ressources pour le long terme.