Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Septembre 2013

Facteurs de cybersécurité à considérer par la direction

Conseils à l'intention du gouvernement du Canada

ITSB-67

Introduction

Les ministères du gouvernement du Canada (GC) ont recours à des systèmes d'information pour soutenir leurs activités opérationnelles. Ces systèmes interconnectés font souvent l'objet de sérieuses menaces susceptibles d'influer négativement sur leurs activités en compromettant la confidentialité, l'intégrité ou la disponibilité de leurs systèmes et de leurs biens de technologie de l'information (TI). L'appui de la haute direction est vital à la protection continue des applications administratives, des biens d'information et des infrastructures de TI. Le présent bulletin identifie les principales questions qui permettront d'orienter les discussions de haut niveau entre la direction et l'équipe de la Sécurité des TI en vue de renforcer la sécurité nationale, de protéger l'information sensible du GC et d'assurer la réalisation des objectifs de mission de leur ministère.

Public visé

Le présent bulletin vise plus particulièrement les cadres supérieurs (non-TI), les dirigeants principaux de l'information, les agents de sécurité des ministères et les cadres supérieurs qui participent aux processus décisionnels en matière de sécurité des TI.

Le contexte de la menace

Les menaces liées aux courriels constituent le plus important facteur de cybermenace auquel sont confrontés les réseaux du GC puisqu'elles peuvent mener à la compromission généralisée du réseau et à l'exfiltration de données. Les auteurs de cybermenaces cherchent à collecter secrètement des données sensibles à partir des systèmes d'information ou tentent de causer le déni, la dégradation, l'interruption ou la destruction de ces systèmes.

Les maliciels, ou logiciels malveillants, sont les outils les plus communément utilisés pour accéder à des réseaux dans le but d'y voler des renseignements ou d'interrompre les activités opérationnelles. Ils peuvent également mener à la création d'un point d'entrée dans un réseau; une fois le point d'entrée en place, un auteur de menace est en mesure d'extraire des renseignements susceptibles d'être utilisés dans le cadre de cyberintrusions ciblées ou de servir à des intérêts stratégiques. Il est par ailleurs possible que votre ministère soit ciblé ou compromis à seule fin d'accéder au réseau d'un autre ministère ou partenaire en exploitant des connexions de confiance.

La méthode la plus souvent utilisée pour répandre des programmes malveillants par courriel est le harponnage. Le CSTC a publié récemment un bulletin intitulé Identification des courriels malveillants (ITSB-100) qui décrit le harponnage comme une tactique qui emploie les techniques d'ingénierie sociale pour façonner des courriels malveillants en fonction de la profession, des intérêts ou des caractéristiques propres aux destinataires. Les courriels de harponnage utilisent des renseignements qui semblent crédibles aux yeux des destinataires en vue de les inciter à ouvrir le courriel et cliquer sur le lien qui y est intégré.

Facteurs de cybersécurité à considérer par la direction

Les cybermenaces deviennent de plus en plus ciblées et sophistiquées; une sécurité inadéquate en matière de TI peut donc mener à une augmentation du nombre d'incidents fructueux liés à la cybersécurité. Pour les organismes, ces incidents peuvent avoir des répercussions directes et importantes sur la confidentialité, l'intégrité ou la disponibilité des systèmes du GC et des biens de TI. Une évaluation appropriée des risques d'atteinte à la sécurité propres à votre organisme permettra de suppléer à vos faiblesses.

1. **Un incident de cybersécurité grave peut coûter cher à votre organisme.**

   Avec l'augmentation de la fréquence et de la complexité des cyberintrusions qui viennent compromettre les réseaux informatiques des ministères, une Sécurité des TI efficace peut vous aider à éviter les coûts directs de

nettoyage ainsi que des coûts indirects, tels que les temps d'arrêt, la perte de productivité, l'atteinte à la réputation de votre organisme et la perte de confiance en celui-ci.

Êtes-vous au courant des incidents de cybersécurité qui surviennent au sein de votre organisme?

> Dans un rapport de 2013 traitant du renseignement sur les cybermenaces, les études de cas menées par Solutionary, Inc. ont révélé que les organismes consacraient jusqu'à 6 500 $ US par heure à la reprise de leurs activités lors d'une attaque par déni de service distribué (DDoS) et qu'il leur fallait jusqu'à 30 jours pour remédier à des intrusions de programmes malveillants à un coût de 3 000 $ US par jour. Ces coûts n'incluent pas les pertes de revenus découlant de l'indisponibilité des systèmes.

2. Un auteur de menace peut tirer parti de l'accès à vos renseignements.

Le Canada est une cible alléchante pour les auteurs de cybermenaces en raison de sa richesse, de ses ressources et des relations diplomatiques qu'il entretient avec ses partenaires. Le renseignement recueilli par les auteurs de cybermenaces peut servir à des intérêts économiques, politiques et technologiques. Le même renseignement peut également être utilisé dans le cadre de cyberintrusions à grande échelle contre des sociétés publiques et privées. Il est important de tenir compte de la valeur de vos renseignements dans leur ensemble, et non seulement de la valeur unitaire des documents. Un auteur de menace peut tirer avantage de ce qu'il a appris sur les caractéristiques de votre réseau pour planifier de futures intrusions.

Recevez-vous des évaluations des dommages liés aux cyberincidents qui surviennent au sein de votre organisme?

Avez-vous votre mot à dire pour ce qui est de déterminer quelle information est la plus importante pour votre organisme et exige une protection accrue?

3. Des contrôles doivent être mis en œuvre pour vous protéger des menaces.

L'ensemble de votre organisme peut tirer avantage d'un programme de sécurité des TI exhaustif axé sur la protection contre les menaces, que ce soit la haute direction, les unités organisationnelles ou les employés. Il est impératif que la direction s'assure de mettre en œuvre des procédures et des politiques clairement définies, de former adéquatement les employés et d'avoir recours à des analyses indépendantes.

La sécurité est un processus continu qui doit sans cesse s'adapter pour répondre aux demandes d'un environnement de menaces en constante évolution. Les techniques de sécurité des TI se perfectionnent au même rythme que s'orchestrent des attaques de plus en plus sophistiquées et ciblées. Aucune solution miracle ne peut protéger en tous points votre ministère contre les cyberintrusions; la cybersécurité est un processus itératif qui permet de gérer le risque à un niveau acceptable. C'est dans le but d'aider votre ministère à gérer le risque que le CSTC a publié le document intitulé Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33). Discutez de l'ITSG-33 avec les membres de l'équipe de Sécurité des TI de votre ministère et encouragez-les à suivre les cours sur la gestion des risques offerts par le Centre de formation en sécurité des TI du CSTC.

Votre équipe de Sécurité des TI peut mettre à profit Les 35 mesures d'atténuation les plus efficaces du CSTC (ITSB-89A) ainsi que les normes et les meilleures pratiques de l'industrie pour protéger vos systèmes et détecter des problèmes potentiels. Le bulletin ITSB-89A et l'approche à la cybersécurité fondée sur la gestion du risque vous aideront à assurer une gestion complète et rentable des cybermenaces.

Savez-vous si votre organisme met en place des pratiques judicieuses en matière de sécurité des TI?

4. La culture de votre organisme doit inciter les employés à faire appel à des techniques de sécurité rigoureuses.

La sécurité de l'information, c'est l'affaire de tout le personnel de votre organisme. La responsabilité des employés doit être clairement définie, communiquée et soutenue par une formation et une sensibilisation efficaces. Il suffit

d'ouvrir une seule pièce jointe dans un courriel malveillant ou d'accéder à un seul site Web mal intentionné pour compromettre l'ensemble de votre réseau. La continuité des activités dans le contexte actuel de la cybermenace repose essentiellement sur la rigueur et l'engagement des employés. Il est donc impératif que la haute direction mise sur la sensibilisation et l'intègre à son cadre stratégique.

La protection de l'information est-elle au cœur des préoccupations de tous les employés?

5. **Il est nécessaire d'élaborer des politiques et des procédures qui décrivent précisément comment intervenir en cas d'incident de cybersécurité.**

   Tous les ministères seront un jour victimes d'un cyberincident; il est donc important de mettre en place les politiques et procédures appropriées pour intervenir en temps opportun. Le fait de connaître les menaces et vulnérabilités propres à chaque organisme peut aider à limiter, voire éviter les atteintes aux biens des TI. Le CSTC propose des rapports spécialisés sur la connaissance de la cybersituation qui vous aideront à mieux comprendre le contexte de la menace.

   Recevez-vous des rapports du CECM du gouvernement du Canada en lien avec votre organisme?

Conclusion

La cybersécurité repose essentiellement sur le soutien apporté par la haute direction. Cette dernière doit élaborer une stratégie de gestion des risques et définir les niveaux acceptables de risque de manière à répondre aux besoins organisationnels du ministère, comme l'établissement des priorités et l'affectation des ressources. Une bonne communication entre la direction et l'équipe de la Sécurité des TI est primordiale et peut contribuer à sensibiliser le personnel aux risques actuels et aux éventuelles répercussions sur les opérations. Les risques ne peuvent être évalués par les spécialistes des TI sans une bonne compréhension du point de vue du propriétaire opérationnel quant à la valeur de l'information. Les priorités en matière de sécurité peuvent ainsi être établies et les ressources affectées en conséquence. Les gestionnaires sont responsables du « I » dans TI. Veillez donc à faire partie du processus de décisions pour ce qui est des risques liés aux TI.

Autres renseignements

Pour les questions d'ordre général au sujet de la sécurité des TI, veuillez envoyer un courriel à itsclientservices@cse-cst.gc.ca.