UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide de mise en place d'un programme de formation et de sensibilisation à la cybersécurité

2024

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIÈRES

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

INTRODUCTION

Le guide NIST SP 800-50r1, intitulé « *Building a Cybersecurity and Privacy Learning Program* », propose un cadre structuré pour créer et gérer un programme de formation et de sensibilisation à la cybersécurité et à la protection de la vie privée. Ce programme vise à renforcer la culture de sécurité au sein des organismes, à promouvoir une meilleure gestion des risques liés à l'information et à développer des compétences en matière de cybersécurité et de protection des données.

PROCESSUS DU PROGRAMME DE FORMATION ET DE SENSIBILISATION

Pour assurer le succès du programme de formation et de sensibilisation en cybersécurité, il est crucial de le piloter de manière proactive tout au long de son cycle de vie. Cela signifie que le responsable doit constamment ajuster le programme en fonction des évolutions internes et des menaces externes.

Le responsable du programme doit définir clairement les objectifs, discuter avec les parties prenantes clés, et s'assurer que chaque décision est documentée et validée. Cette rigueur permet d'aligner le programme avec les priorités stratégiques de l'établissement, tout en restant flexible pour répondre aux défis émergents. En adoptant une approche basée sur des retours réguliers et des indicateurs de performance tout au long de l'année, le programme permettra de renforcer la culture de cybersécurité.

Les phases essentielles pour construire et gérer un programme complet incluent : planification et stratégie, analyse et conception, développement et mise en œuvre ainsi que l'évaluation et l'amélioration continue.

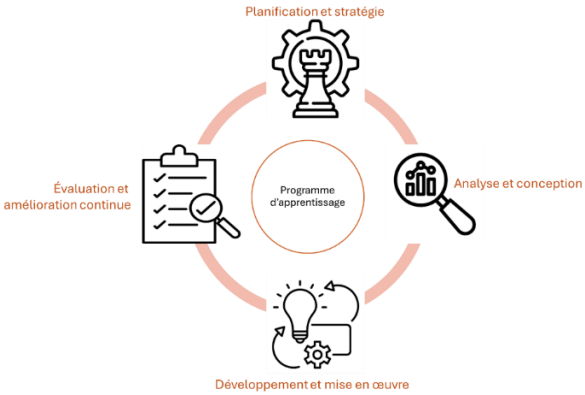

Figure 1 Processus du programme de formation et de sensibilisation

PLANIFICATION ET STRATÉGIE

VISION ET OBJECTIFS STRATÉGIQUES

Avant de commencer toute planification, il est essentiel de définir une vision claire de ce que le programme cherche à accomplir. La vision doit être alignée avec la mission globale de l'établissement et se focaliser sur la création d'une culture de sécurité.

Les objectifs stratégiques consistent à :

- Réduire les incidents de sécurité liés au facteur humain (ex. : incidents d'hameçonnage, erreurs de manipulation de données).
- Améliorer la compréhension des utilisateurs sur les politiques de sécurité et de confidentialité.
- Encourager l'adoption de bonnes pratiques de sécurité à travers des formations continues et des rappels réguliers.

PARTIES PRENANTES

Pour garantir la réussite du programme, il est crucial d'identifier toutes les parties prenantes et de comprendre leurs rôles et responsabilités. Voici une liste, sans s'y limiter :

- Direction : soutenir le programme en allouant des ressources et en communiquant son importance à tout l'établissement.
- Chef de la sécurité de l'information organisationnelle (CSIO) : superviser la conception et le déploiement du programme, en s'assurant qu'il est conforme aux normes de sécurité.
- Responsables des ressources humaines : assurer l'intégration du programme dans le parcours de formation des nouveaux employés.
- Gestionnaires d'équipes : relayer le message et motiver leur équipe à suivre les formations.

ÉLABORATION DES BESOINS EN FORMATION

Avant de définir la stratégie de formation, il est nécessaire de cartographier les risques et d'analyser les besoins de formation. Cela comprend :

- Identifier les menaces actuelles.
- Cartographier les lacunes de connaissance en fonction des rôles dans l'établissement.
- Évaluer le niveau de maturité de la culture de sécurité de l'établissement.
- Définir les priorités : type de formation urgente et population cible ayant un besoin d'une formation plus approfondie.

INDICATEURS DE PERFORMANCE

Les indicateurs clés de performance (KPIs) aident à mesurer le succès du programme et à ajuster les actions en conséquence. Quelques exemples de KPIs pertinents :

- Taux de participation aux formations : nombre d'utilisateurs qui ont suivi les sessions proposées.
- Résultats aux tests de connaissances : évaluer les progrès des utilisateurs.
- Réduction du nombre d'incidents liés au comportement humain (ex. : clics sur des liens d'hameçonnage).
- Indice de satisfaction des employés vis-à-vis du programme.

STRATÉGIE DE COMMUNICATION

La stratégie de communication est essentielle pour que le programme atteigne efficacement toutes les équipes de l'établissement. Il s'agit de transmettre les messages de manière claire, régulière et ayant de l'impact.

- Définir l'audience cible : segmenter les utilisateurs en groupes (utilisateurs standard, équipes techniques, dirigeants) et adapter les messages à leurs rôles et responsabilités.
- Développer des messages clés : créer des messages simples et adaptés aux risques.
- Choisir les canaux : utiliser un mélange de courriels, d'affiches, de vidéos, et de plateformes de communication internes pour maximiser l'impact.
- Calendrier de communication : planifier des rappels réguliers et synchroniser les campagnes avec des événements clés comme le mois de la cybersécurité.
- Encourager l'interaction : utiliser des questionnaires, des simulations d'attaques et des défis pour rendre la sensibilisation engageante et interactive.

PLANIFICATION BUDGÉTAIRE

La planification et la stratégie du programme doivent inclure un budget dédié pour couvrir :

- Le développement de contenu (vidéos, modules de cyberapprentissage, supports papier).
- Les sessions de formation en présentiel ou virtuelles.
- Les exercices pratiques.
- La technologie nécessaire.

ANALYSE ET CONCEPTION

La phase d'analyse et de conception permet de comprendre les besoins de formation spécifiques de l'établissement, de cartographier les risques associés et de concevoir des solutions adaptées aux différents groupes cibles.

ÉVALUATION DES BESOINS

La première étape consiste à réaliser une analyse approfondie des besoins de l'établissement en matière de cybersécurité. Cette évaluation doit inclure :

- L'identification des menaces : examiner les types de menaces les plus courants dans le secteur universitaire (hameçonnage, logiciel de rançon, fuites de données).
- La cartographie des risques : évaluer les risques auxquels chaque département ou fonction est exposé.
- L'analyse des incidents passés : étudier les incidents précédents pour identifier les failles humaines récurrentes et en tirer des leçons.
- Les enquêtes internes : recueillir les perceptions des employés via des questionnaires ou des entretiens pour identifier les lacunes en matière de formation et de sensibilisation.

SEGMENTATION EN GROUPES

Cette étape repose sur une segmentation précise des différents types d'utilisateurs au sein de l'établissement. Chaque groupe aura des besoins de formation distincts basés sur ses responsabilités et son niveau d'accès aux informations sensibles.

DÉFINIR LES OBJECTIFS

Les objectifs doivent être clairement définis pour chaque segment et peuvent consister à des :

- Objectifs généraux : expliquer les risques de cybersécurité, les principes de base de la protection des données et l'importance de suivre les protocoles.
- Objectifs spécifiques : Par exemple : reconnaître un courriel d'hameçonnage, appliquer correctement les politiques de gestion des mots de passe ou réagir en cas d'incident de sécurité.

SCÉNARIOS DE FORMATION

Les scénarios de formation permettent de transposer les risques théoriques en situations pratiques que les utilisateurs peuvent rencontrer au quotidien. Voici quelques types de scénarios à inclure :

- Scénarios d'hameçonnage simulés : envoyer des courriels simulés pour tester la réaction des utilisateurs.
- Exercices de gestion de crise : simuler une violation de données et évaluer la réaction des équipes.
- Cas pratiques basés sur des incidents réels : utiliser des incidents survenus dans d'autres établissements comme base de réflexion et d'apprentissage.

Les scénarios doivent être engageants, réalistes et adaptés à chaque groupe cible pour rendre l'expérience de formation pertinente et mémorable.

MATRICE DES COMPÉTENCES

Une matrice des compétences est un outil qui permet de cartographier les compétences requises pour chaque rôle par rapport à celles actuellement maîtrisées. Cela aide à identifier les écarts de formation et à prioriser les sessions selon les besoins.

- Compétences de base : maîtrise des bonnes pratiques de cybersécurité (gestion des mots de passe, protection des appareils).
- Compétences intermédiaires : compréhension des menaces spécifiques (techniques d'hameçonnage, attaques par ingénierie sociale).
- Compétences avancées : réponse aux incidents, gestion de crise, audits de sécurité.

Cette matrice doit être régulièrement mise à jour pour s'adapter aux nouvelles menaces et évolutions des responsabilités des utilisateurs.

DÉVELOPPEMENT ET MISE EN ŒUVRE

La phase de développement et de mise en œuvre est essentielle pour traduire les objectifs stratégiques définis lors de la phase d'analyse et de conception en actions concrètes. Cette phase implique la création de contenus pédagogiques, la planification logistique des sessions de formation et le déploiement du programme auprès de l'ensemble des parties prenantes de l'établissement. L'objectif est de veiller à ce que les concepts de sécurité soient bien compris et intégrés par tous les utilisateurs.

CONCEPTION DU CONTENU PÉDAGOGIQUE

Le développement de contenus doit être planifié pour répondre aux besoins de formation identifiés et aux objectifs définis. Il sera important de créer des supports de formation qui sont à la fois engageants, pertinents et adaptés aux différents niveaux de connaissance des utilisateurs.

RESSOURCES EXTERNES

Dans certains cas, il peut être plus efficient d'acquérir des contenus de formation auprès de fournisseurs externes, surtout si le programme doit couvrir des sujets techniques complexes.

Il convient de considérer les critères d'évaluation suivants :

- Conformité avec les normes de sécurité et de protection des données.
- Qualité du contenu : évaluer la profondeur des informations et la clarté des supports.
- Adaptabilité : le contenu doit pouvoir être personnalisé pour inclure les politiques de l'établissement.
- Processus d'intégration : avant de lancer le contenu auprès de tous les utilisateurs, effectuez un test sur un groupe restreint pour valider la pertinence et l'efficacité du matériel.

PLAN DE DÉPLOIEMENT

Cette étape permet de déterminer le moment opportun et la séquence de la mise en œuvre du programme pour maximiser l'impact.

Pour établir le calendrier, il est nécessaire de prioriser les groupes critiques (par exemple, les responsables de la sécurité et les administrateurs système) avant de déployer le programme aux utilisateurs standard. Il sera important de planifier des sessions de rappel à intervalles réguliers (par exemple, trimestriel) pour maintenir un haut niveau de vigilance.

Afin de gérer efficacement la logistique, il convient d'envisager l'utilisation d'un LMS (Learning Management System) pour gérer les inscriptions, le suivi de la progression et la distribution des modules de formation.

Il sera important de prévoir des sessions en présentiel ou des webinaires pour les modules complexes nécessitant des interactions en direct.

LANCEMENT DU PROGRAMME

La phase de lancement doit être accompagnée d'une campagne de communication pour maximiser la participation et susciter l'intérêt des utilisateurs.

Parmi les stratégies de communication, on peut citer :

- Annonce officielle par la direction pour démontrer l'importance du programme.
- Utiliser différents canaux (courriels, affiches, réunions d'équipe) pour informer tous les niveaux de l'établissement.
- Mettre en place une boîte à questions ou des sessions d'échanges pour répondre aux préoccupations des employés.

SUIVI DE LA PARTICIPATION

Cette étape vise à suivre la participation et à intervenir pour garantir que les objectifs sont atteints.

Voici quelques indicateurs clés :

- Taux de participation : mesurer le pourcentage d'utilisateurs ayant suivi les formations requises.
- Résultats des tests : évaluer la compréhension et l'assimilation des concepts clés.
- Retour des utilisateurs : Recueillir des retours réguliers pour ajuster le contenu.

ÉVALUATION ET AMÉLIORATION CONTINUE

Cette phase vise à garantir que le programme reste pertinent, efficace et aligné avec les objectifs stratégiques de l'établissement. Elle permet non seulement de mesurer l'impact du programme, mais aussi d'identifier les points à améliorer pour renforcer les comportements sécuritaires à long terme.

MÉTRIQUES

L'évaluation de l'efficacité d'un programme commence par la définition de métriques claires. Ces indicateurs permettent de quantifier les progrès réalisés, d'identifier les lacunes, et de guider les futures améliorations.

- Taux de participation : pourcentage d'employés ayant complété les modules de formation. Comparer ce taux entre les départements pour identifier les groupes moins engagés.
- Résultat des évaluations : scores obtenus aux questionnaires et tests finaux pour évaluer la compréhension, pourcentage d'utilisateurs atteignant le score minimum requis.
- Taux de conformité : mesurer le respect des politiques internes de sécurité (ex. : fréquence de changement des mots de passe, utilisation de l'authentification multifacteur).
- Réduction des incidents de sécurité liés au facteur humain : suivi des incidents tels que les clics sur des liens d'hameçonnage, les violations de données causées par une mauvaise manipulation d'informations.
- Retour des participants : taux de satisfaction global du programme, retour qualitatif sur l'efficacité, la pertinence et la présentation du contenu.

ÉVALUATION RÉGULIÈRE

L'évaluation du programme ne doit pas se limiter à une vérification annuelle. Elle doit inclure des évaluations régulières pour suivre les progrès et ajuster les actions en fonction des résultats obtenus.

- Évaluations trimestrielles : mesurer l'évolution des connaissances et l'application des bonnes pratiques, réaliser des campagnes d'hameçonnage pour évaluer la vigilance des utilisateurs.

- Organiser des exercices de réponse à incident pour les équipes techniques afin d'évaluer leur capacité à détecter, contenir et résoudre les incidents.
- Revues annuelles : réaliser une analyse approfondie pour vérifier si les objectifs stratégiques ont été atteints et comparer les performances d'une année à l'autre pour mesurer l'impact du programme à long terme.

AJUSTEMENT DES OBJECTIFS

Les résultats de l'évaluation doivent être utilisés pour ajuster les objectifs du programme et adapter le contenu en fonction des nouvelles menaces ou des changements de politique.

- Mise à jour des scénarios : modifier les simulations d'attaques en fonction des nouvelles techniques utilisées par les attaquants (ex. : attaques par harponnage, nouvelles failles de sécurité).
- Adaptation aux nouvelles réglementations : si de nouvelles exigences légales ou de conformité sont introduites, s'assurer que les modules sont rapidement mis à jour pour inclure ces changements.
- Obligation en fonction des résultats : si un département particulier montre un taux élevé de clics sur les simulations d'hameçonnage, renforcer les sessions de formation pour ce groupe.

CYCLE D'AMÉLIORATION CONTINUE

Pour garantir la pérennité et l'efficacité du programme, il est essentiel de mettre en place un cycle d'amélioration continue basé sur les résultats et les évolutions de l'environnement de sécurité.

- Établir de nouveaux objectifs basés sur les résultats de l'évaluation.
- Mettre en œuvre les ajustements et les nouvelles initiatives.
- Déployer les changements auprès de tous les utilisateurs.
- Mesurer l'efficacité des changements et ajuster de nouveau.

Le cycle d'amélioration continue garantit que le programme reste dynamique, proactif et toujours aligné avec les priorités de l'organisation.

RECOMMANDATIONS DU NIST

Le nombre, la fréquence et la durée des sessions de formation et de sensibilisation dépendent du contexte de l'établissement, des objectifs de sensibilisation, du type d'audience et du niveau de maturité en matière de sécurité de l'établissement. Toutefois, voici quelques recommandations générales basées sur les bonnes pratiques :

NOMBRE DE SESSIONS.

- Annuel : un programme complet de sensibilisation est recommandé une fois par an pour l'ensemble des utilisateurs.
- Sessions thématiques : d'autres sessions peuvent être organisées tout au long de l'année sur des sujets spécifiques (p. ex. : hameçonnage, gestion des mots de passe, sécurité des courriels, protection des données).
- Pour les nouveaux utilisateurs : une session d'intégration dédiée à la sécurité pour chaque nouvelle recrue.

FRÉQUENCE

- Sessions régulières : recommandé d'avoir une session de sensibilisation générale au moins une fois par an.
- Microsessions trimestrielle ou bimensuelle : des rappels sous forme de courtes formations (15 à 30 minutes) ou d'ateliers peuvent être organisés tous les trimestres pour renforcer les messages.
- Simulations d'hameçonnage : idéalement, une à deux fois par trimestre pour évaluer la réaction des utilisateurs et ajuster la formation.

DURÉE

- Sessions principales : de 45 minutes à 1 heure pour des formations plus générales.
- Sessions spécifiques : 30 à 45 minutes pour des sujets particuliers (ex. : sensibilisation à la PRP, gestion des incidents).
- Microformations : Moins de 15 minutes pour des rappels ou des formations.

TLP : VERT (DIFFUSION PERMISE)

RÉFÉRENCES

https://csrc.nist.gov/News/2024/nist-publishes-sp-800-50-revision-1 Building a Cybersecurity and Privacy Learning Program: NIST Publishes SP 800-50r1

PR.AT: Awareness and Training - CSF Tools NIST Cybersecurity Framework v1.1

PR.AT: Awareness And Training - CSF Tools NIST Cybersecurity Framework v2.0

RÉVISIONS

Date	Action	Auteur	Version
2024-11-28	Révision linguistique	Joanne Lussier	1.0
2024-11-25	Intégration des commentaires	Mehdi Tanazefti CESI de l'UQ	0.9
2024-10-07	Version initiale	Mehdi Tanazefti CESI de l'UQ	0.8