Éducation Québec
Direction de l'accès à l'information et des plaintes

Québec, le 17 juin 2021

PAR COURRIEL

Objet : Demande d'accès à des documents administratifs
Notre dossier : 16310/20-397

Monsieur,

La présente a pour objet de faire le suivi de votre demande d'accès, visant à obtenir :

- tous rapports ou autres documents sur l'état de préparation aux cyberattaques et/ou la capacité opérationnelle du Ministère et des centres de services scolaires à réagir aux atteintes à la protection des données, du 1er janvier 2017 à aujourd'hui, le 10 mars 2021;
- tous rapports ou autres documents relatifs à toute atteinte à la protection des données qui ont eu lieu depuis le 1er janvier 2018 au Ministère ou aux centres de services scolaires.

Vous trouverez ci-annexé les documents pouvant répondre à votre demande.

Nous vous invitons également à consulter les informations concernant le vol de données qui ciblait les enseignants, diffusées à l'adresse suivante :

https://www.quebec.ca/education/vol-donnees-ministere-education

Une vérification étant en cours au sujet de cet incident, certains documents produits dans le cadre de cette démarche ne peuvent vous être acheminés en vertu des articles 14, 28, 41 et 127 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (RLRQ, chapitre A-2.1, ci-après « La Loi »).

De plus, certains documents ne peuvent vous être transmis étant donné que ceux-ci présentent des projets et/ou contiennent des analyses, des avis, des recommandations et des informations qui pourraient compromettre la sécurité des systèmes informatiques du Ministère. Cette décision s'appuie sur les articles 9, 14, 22, 29, 37 et 39 de la Loi. Également, des documents comportant des renseignements personnels confidentiels sont retenus en vertu des articles 53, 54, 56 et 59 de la Loi.

… 2

Édifice Marie-Guyart
1035, rue De La Chevrotière, 27e étage
Québec (Québec) G1R 5A5
Téléphone : 418 528-6060
Télécopieur : 418 643-1602
acces@education.gouv.qc.ca

D’autres documents produits par les centres de services scolaires ou par les commissions scolaires ne peuvent vous être transmis puisque leur accessibilité doit être évaluée par ces organismes. En vertu de l’article 48 de la Loi, nous vous invitons à formuler votre demande auprès des responsables de l’accès de ces organismes dont vous trouverez les coordonnées à l’adresse suivante :

https://www.cai.gouv.qc.ca/liste-des-organismes-assujettis-et-des-responsables-de-lapplication-de-la-loi-sur-lacces/

Enfin, des documents détenus par le Ministère ne peuvent vous être accessibles en vertu de l’article 34 de la Loi, car ce sont des « documents du cabinet du ministre » ou ont été produits pour son compte.

Vous trouverez en annexe une reproduction des articles de la Loi précédemment.

Conformément à l’article 51 de la Loi, nous vous informons que vous pouvez demander la révision de cette décision auprès de la Commission d’accès à l’information. Vous trouverez en annexe une note explicative à cet effet.

Veuillez agréer, Monsieur, nos salutations distinguées.

La responsable de l’accès aux documents,

Originale signée

Ingrid Barakatt
IB/JC/mc

p.j. 9

Québec

N° : 2020-002.02
Date : 2020-11-18

Instruction relative à la déclaration des incidents de type hameçonnage

C CD

Instruction relative à la déclaration des incidents de type hameçonnage

Objet de l'instruction

La présente instruction décrit une démarche à suivre afin d'identifier une attaque de type hameçonnage et de la déclarer auprès du COCD.

Champ d'application

- Le ministère de l'Éducation et le ministère de l'Enseignement supérieur
- Tous les établissements du réseau de l'éducation

Définitions et terminologies

Incident de type hameçonnage: On entend par « Incident de type hameçonnage » toute tentative frauduleuse exploitant un composant du système d'information (messagerie électronique, téléphone, plateforme de partage, etc.) et demandant à un utilisateur de cliquer sur un lien, de télécharger une pièce jointe ou de divulguer une information confidentielle.
Harponnage : En anglais : « spear phishing ». C'est un type d'attaque d'hameçonnage caractérisé par le fait de cibler un individu ou un ensemble d'individus spécifique, tel que les cadres supérieurs de l'organisme attaqué (président, directeur, etc.).
Courriel suspect : Un courriel jugé d'être le vecteur d'une attaque d'hameçonnage.

Règles de gestion:

- Tout utilisateur qui reçoit un courriel suspect ou n'importe quelle forme d'hameçonnage doit déclarer un incident de type hameçonnage.
- Tout incident d'hameçonnage doit être signalé au COCD par le COGI/CSGI à travers le formulaire de déclaration d'incident, après avoir effectué les vérifications indiquées dans le présent document.
- Les utilisateurs doivent être sensibilisés sur les évènements et incidents de sécurité à remonter.

L'hameçonnage :

Qu'est-ce que l'hameçonnage?

L'hameçonnage est une forme d'attaque par ingénierie sociale, qui vise à exploiter la confiance des utilisateurs pour les convaincre de révéler des informations sensibles, télécharger une pièce jointe ou cliquer sur un lien malveillant.
Les objectifs d'une attaque d'hameçonnage peuvent varier entre le vol des données ou l'injection d'un logiciel malveillant visant la compromission de la machine.

Comment cela fonctionne?

Il existe plusieurs méthodes pour mener une attaque de type hameçonnage. Selon leurs objectifs, les cybercriminels peuvent exploiter différents vecteurs d'attaque pour cibler un organisme. Les courriels, les SMS, les appels téléphoniques, les plateformes de partage, les réseaux sociaux sont tous des vecteurs qui peuvent être exploités pour mener une attaque d'hameçonnage.

Selon le vecteur d'attaque exploité, le cybercriminel peut utiliser une des méthodes suivantes :

1) Convaincre sa victime de lui fournir des informations sensibles directement.
2) Convaincre sa victime de cliquer sur un lien redirigeant vers une page usurpée ou malveillante.
3) Convaincre sa victime de télécharger et exécuter une pièce jointe malveillante.

Quelles sont les informations ciblées ?

Plusieurs types de données peuvent être ciblées par les attaques de type hameçonnage. Les informations suivantes sont les plus ciblées :

- Le nom d'utilisateur et le mot de passe pour des comptes personnels ou professionnels.
- Les informations d'identité personnelle: Le nom, l'adresse de domicile, le NAS, etc., qui peuvent être utilisées pour le vol d'identité.
- Les adresses courriels et contacts de vos collègues qui peuvent être utilisés pour d'autres attaques d'hameçonnage.
- Les informations confidentielles de l'organisme.
- Les informations bancaires d'utilisateur.

Comment se protéger de l'hameçonnage?

L'utilisateur est l'élément clé dans ce type d'attaques. En effet, la protection d'un organisme contre les attaques d'hameçonnage et leurs conséquences repose sur les bons réflexes de ses utilisateurs. La meilleure façon de se protéger est de sensibiliser ses utilisateurs pour avoir de bons réflexes et suivre la démarche décrite dans la présente instruction. Voici quelques points à prendre en considération dans le cadre de la sensibilisation de ses utilisateurs:

- Toujours vérifier l'identité de votre interlocuteur. Utiliser un autre canal de communication en cas de doute (téléphone, SMS, etc.).
- Réfléchir à deux fois avant de cliquer sur des liens, télécharger des fichiers ou ouvrir des pièces jointes dans des courriels (ou sur les médias sociaux), même si cela semble provenir d'une source fiable et connue.
- S'assurer que l'adresse du site (son URL) correspond bien à celui vers lequel vous serez redirigé et que c'est bien l'adresse habituelle de l'interlocuteur ou l'organisme concerné.
- Adopter la règle d'or de ne jamais communiquer vos informations personnelles (code secret, coordonnées bancaires, etc.), par téléphone ou courriel, à qui que ce soit.
- Changer régulièrement les mots de passe qui doivent être suffisamment complexes.
- Rester vigilant lorsqu'un courriel demande des actions urgentes.
- En cas de doute, demander l'avis d'une personne tiers.

Description de l'instruction

Afin de couvrir le déroulement d'un incident de type hameçonnage, de son apparition au niveau de l'utilisateur jusqu'à sa déclaration auprès du COCD, la démarche présentée dans cette instruction est divisée en deux parties. La première partie décrit les étapes à suivre par un utilisateur pour identifier et déclarer correctement un incident de type hameçonnage. La deuxième partie présente les principaux éléments à prendre en considération par le COGI/CSGI lors de la déclaration d'un incident de type hameçonnage auprès du COCD.

Côté utilisateur :

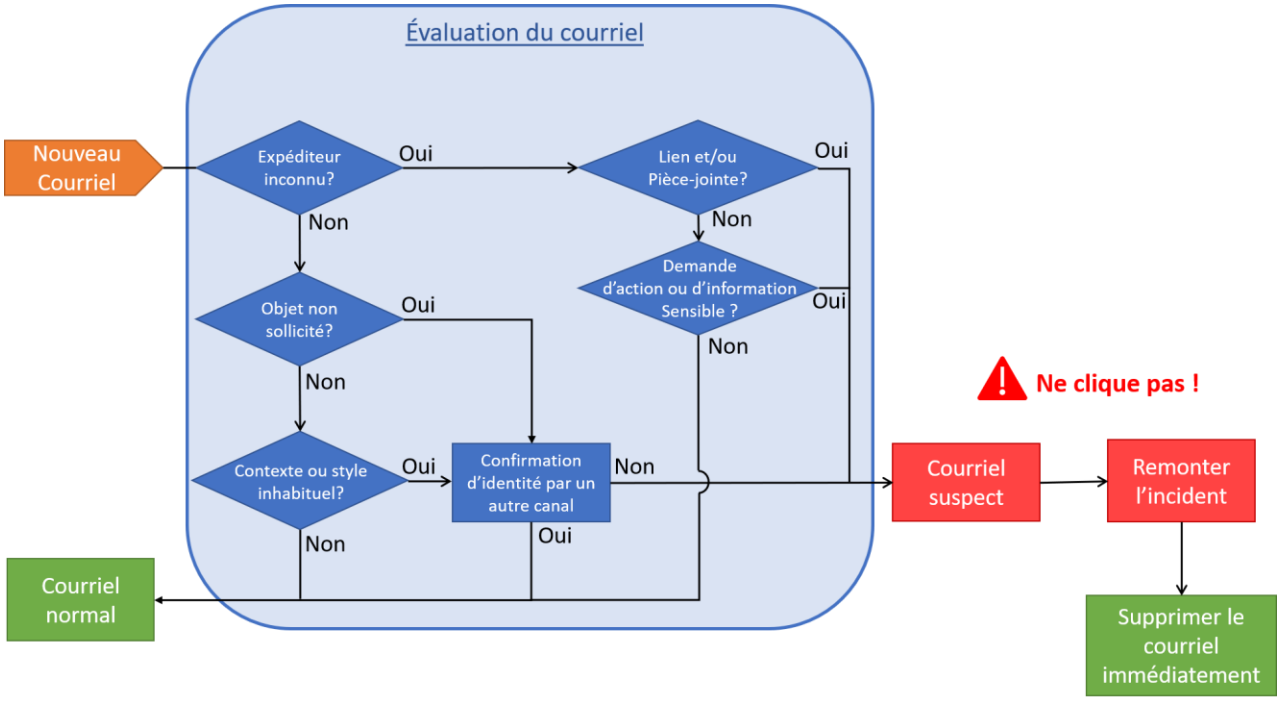
La présente démarche focalise sur l'hameçonnage par courriel, puisque c'est la méthode la plus utilisée. En effet, l'utilisateur doit être très attentif avec les courriels qu'il reçoit sur sa boite professionnelle et personnelle. Chaque utilisateur doit être capable d'évaluer ses courriels, afin d'identifier les courriels suspects et les déclarer au COGI/CSGI. L'utilisateur doit vérifier, dans un premier lieu, l'identité de l'expéditeur:

- Si l'expéditeur est inconnu, l'utilisateur doit vérifier la présence d'une pièce jointe ou d'un lien attaché au courriel. Si c'est le cas, il doit remonter un incident de type hameçonnage en joignant une copie du courriel suspect et le supprimer immédiatement. En cas d'absence de pièce jointe et de lien,

l'utilisateur doit vérifier dans le corps du courriel si l'expéditeur demande une action (envoi d'argent, etc.) ou une information sensible (NAS, etc.). Dans ce cas, le courriel doit être considéré suspect et un incident de type hameçonnage doit être remonté.

- Si l'expéditeur est reconnu par l'utilisateur (collègue, collaborateur interne ou externe), ce dernier doit vérifier l'objet, le contexte et le style d'écriture. S'il détecte des choses inhabituelles ou non sollicitées, il doit confirmer l'identité de l'expéditeur par un autre canal (appel téléphonique, SMS). Si la personne concernée n'a pas confirmé l'envoi de ce courriel, l'utilisateur doit le considérer comme suspect, il doit donc remonter un incident de type hameçonnage en joignant une copie du courriel suspect et le supprimer immédiatement.

Logigramme :



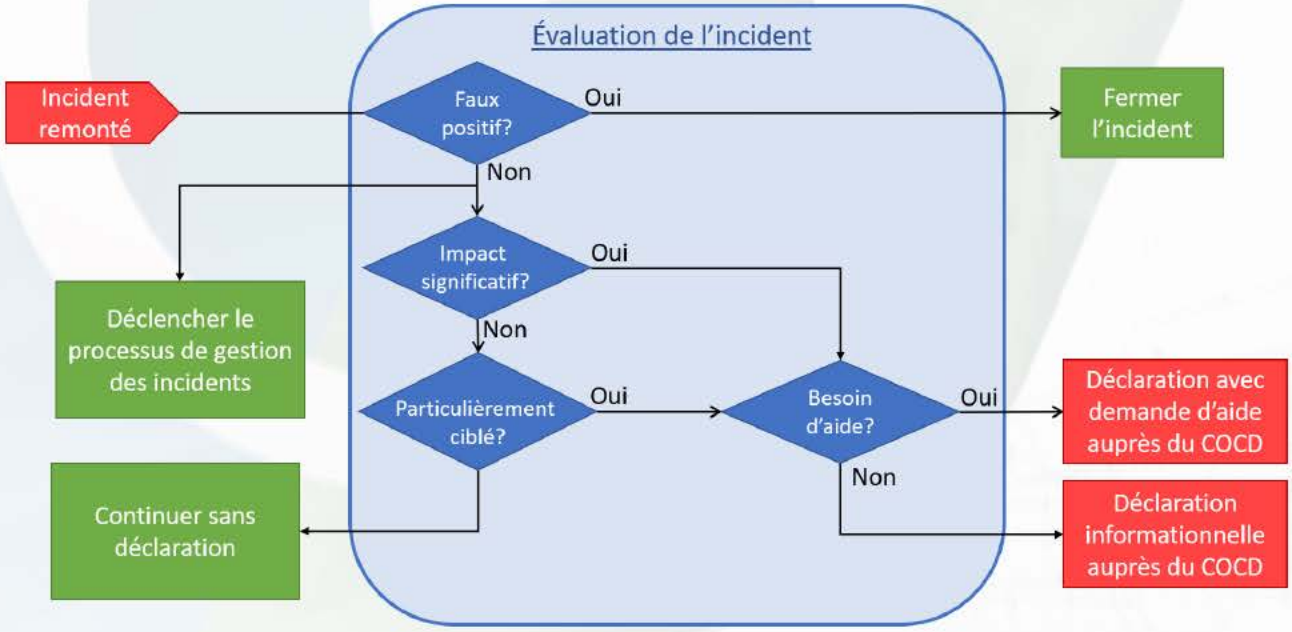
Côté service informatique :

Une fois qu'un incident de type hameçonnage est remonté par un utilisateur, le « service informatique » doit mener une évaluation de cet incident pour vérifier qu'il ne s'agit pas d'un faux positif, avant de lancer le processus de réponse aux incidents et la démarche de déclaration d'incidents auprès du COCD. Le « service informatique » est appelé à évaluer l'impact de chaque incident de type hameçonnage et à distinguer les attaques particulièrement ciblées (les attaques de type « harponnage » (Spear phishing), celles qui ciblent particulièrement le réseau de l'éducation, celles conçues pour une distribution massive d'un logiciel malveillant, etc.). En cas d'impact significatif ou s'il s'agit d'une campagne particulièrement ciblée, l'incident doit être remonté au COCD. En cas de besoin d'une intervention du COCD, le COGI/CSGI doit effectuer une déclaration avec demande d'aide. Si non, il doit effectuer une déclaration à titre informatif seulement.

Selon son niveau de maturité en matière de gestion des incidents de sécurité, chaque organisme va choisir une des deux approches suivantes afin d'effectuer une déclaration efficace d'un incident de type hameçonnage :

- Les organismes et les établissements organisés en matière de sécurité de l'information et de gestion des incidents sont appelés à effectuer l'ensemble de vérifications décrites dans la présente démarche et joindre leur formulaire de déclaration par une synthèse de la situation de l'incident, ainsi qu'une copie du courriel suspect pour des fins d'analyse et d'investigation par le COCD. Ou joindre les indicateurs de compromission (IOCs) liés à l'incident directement.
- Les organismes et les établissements qui ne possèdent pas une organisation suffisante pour analyser ce genre d'incidents doivent rapidement remplir la déclaration et joindre une copie originale du courriel suspect. Le COCD les recontactera en cas de besoin.

Logigramme :



Éducation et Enseignement supérieur Québec	**Instruction du centre opérationnel de cyberdéfense (COCD)**	No : **2020-003.01** Date : **2020-04-08**

Objet de l'instruction

L'objectif de cette instruction est d'introduire le processus d'alerte du COCD ainsi que de décrire les bulletins de sécurité diffusés par le COCD.

Champ d'application

- Tous les établissements du réseau de l'éducation
- Le MÉES

Définitions et terminologies

Actif : On entend par « actif » ou « actif informationnel » tout élément qui a de la valeur pour l'organisme (par exemple : une information, un matériel, un logiciel, etc.).

Cybermenace : Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs informationnels d'un organisme.

Vulnérabilité : Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les actifs ou les activités d'un organisme.

Impact : C'est la conséquence négative d'un incident sur un ou plusieurs actifs informationnels.

Règles de gestion:

- Les organismes du réseau de l'éducation doivent rester vigilants aux bulletins de sécurité du COCD. En cas d'alerte, ils doivent réagir rapidement en appliquant les recommandations du plan d'action proposé.
- Les recommandations proposées doivent être adaptées par chaque organisme à son contexte en évaluant leurs impacts avant de les appliquer.
- Les bulletins de sécurité, produits par le COCD, seront envoyés par courriel à ses interlocuteurs au sein des différents organismes et établissements du réseau de l'éducation.
- Les destinataires de ces bulletins de sécurité peuvent les redistribuer au sein de leurs organismes tout en respectant le niveau de confidentialité de chaque bulletin.
- Selon leur niveau de confidentialité, certains bulletins et leurs mises à jour seront publiés sur le canal « Alerte » dans Teams.

Description de l'instruction

Dans le cadre de sa mission de veille sur les vulnérabilités et les cybermenaces, et afin d'établir des canaux de communication efficaces avec ses interlocuteurs, le COCD vous annonce le lancement de la diffusion de ses propres bulletins d'alerte de sécurité.

Les bulletins d'alerte du COCD s'adressent aux professionnels et aux gestionnaires de la sécurité de l'information au sein des organismes et des établissements du réseau de l'éducation.

En se basant sur des informations collectées de manière fiable et en continu, à l'intérieur du réseau de l'éducation et à l'extérieur, ainsi que sur des analyses poussées de ses experts internes, le COCD produira des alertes et des avis de sécurité. Ces alertes de sécurité peuvent concerner des vulnérabilités récemment découvertes, des cybermenaces détectées par le service de veille du COCD ou des incidents détectés dans un établissement et qui peuvent potentiellement se reproduire dans d'autres établissements du réseau. L'objectif est de vous fournir une synthèse

informative sur les alertes ainsi que de vous offrir un plan d'action avec un ensemble de mesures à mettre en œuvre pour vous protéger.

Afin de faciliter leur lecture, les bulletins de sécurité du COCD seront organisés dans un format unifié. Le tableau 1 décrit la structure d'un bulletin d'alerte de sécurité du COCD.

Référence	MEES-2020-ALE-001
Confidentialité du bulletin	○ Public ● Diffusion interne ● Diffusion restreinte ● Privé
Date de publication	
Titre	
Nature	○ Vulnérabilité ○ Menace ○ Incident
Impact potentiel	○ Négligeable ● Mineur ● Important ● Critique
Statut	☐ Preuve de concept existante ☐ Exploitée sur internet ☐ Exploit publié
Risques	☐ Exécution de code arbitraire à distance ☐ Élévation de privilèges ☐ Déni de service à distance ☐ Atteinte à l'intégrité des données ☐ Atteinte à la confidentialité des données
Synthèse	Une brève synthèse sur le sujet du bulletin d'alerte.
Périmètre concerné	L'environnement technologique et produits concernés.
Détails	Rapport plus détaillé sur le sujet du bulletin d'alerte.
Plan d'action	Recommandations et actions à mettre en place.
Mots clés	
Indicateurs	Indicateurs permettant de détecter la menace si applicable.
Liens externes	Référentiels pour plus de détails.
Bulletins de référence	D'autres bulletins du COCD en relation avec le bulletin actuel.

Tableau 1 : *Structure d'un bulletin de sécurité du COCD*

Dans le but d'adopter le même langage et afin d'éviter toute sorte d'ambigüité, le COCD vous fournit, dans la présente instruction, la définition de chaque terminologie adoptée ainsi que les échelles utilisées dans chaque rubrique de ses bulletins de sécurité.

Le tableau suivant vous fournit l'échelle de gravité d'impacts potentiels adoptée par le COCD.

Négligeable	Impact faible sur les critères de sécurité et sans divulgation de renseignements personnels ou confidentiels.
Mineur	Impact limité mais non négligeable sur les critères de sécurité et sans divulgation des renseignements personnels ou confidentiels.
Important	Impact significatif sur les critères de sécurité avec perte ou divulgation limitée de renseignements personnels ou confidentiels.
Critique	Impact conséquent sur les critères de sécurité avec perte ou divulgation importantes de renseignements personnels ou confidentiels.

Tableau 2 : *Échelle de gravité d'impacts potentiels*

Certains bulletins de sécurité du COCD peuvent contenir des informations confidentielles qui ne doivent pas quitter le réseau de l'éducation ou qui sont destinées à des établissements ou à des individus spécifiques. La redistribution de ces bulletins doit obligatoirement respecter leurs niveaux de confidentialité. À cette fin, le COCD vous fournit une échelle de confidentialité en quatre niveaux. La définition de chaque niveau de confidentialité est décrite dans le tableau 3 ci-dessous :

Public	Bulletin non classifié, il peut être diffusé hors du réseau de l'éducation.
Diffusion interne	Bulletin non public mais diffusable largement au sein du réseau de l'éducation.
Diffusion restreinte	Bulletin contenant des données sensibles à ne diffuser que de façon limitée au sein d'un établissement.
Privé	Bulletin avec des données très sensibles à ne transmettre qu'aux individus légitimes.

Tableau 3 : *Échelle de confidentialité des bulletins du COCD.*

Si le bulletin d'alerte concerne une vulnérabilité découverte dans une des technologies utilisées au sein du réseau de l'éducation, deux rubriques seront ajoutées : la rubrique « Statut » vous indiquera le statut actuel de la vulnérabilité et la rubrique « Risques » vous donne les risques liés à cette vulnérabilité. Il est possible que plusieurs modes soient cochés.

Québec

N° : 2020-004.01
Date : 2020-08-21

Instruction relative à la gestion des comptes à hauts privilèges

CCCD

Instruction relative à la gestion des comptes à hauts privilèges

Objet de l'instruction

L'objectif de cette instruction est de fournir aux établissements des réseaux de l'éducation un ensemble de bonnes pratiques dans la gestion des comptes à privilèges. Le but est de renforcer l'efficacité et la sécurité des contrôles d'accès administratifs aux différentes solutions et plateformes du système d'information.

Champ d'application

- Le Ministère de l'Éducation et le Ministère de l'Enseignement supérieur
- Tous les établissements des réseaux de l'éducation

Définitions et terminologies

Comptes à hauts privilèges : Comptes qui comprennent les comptes d'administrateur, les comptes intégrés et les comptes utilisés pour exécuter des programmes de service. Ils sont des comptes hautement sensibles qu'il faut entourer de mesures de sécurité supplémentaires et contrôler périodiquement.
Comptes utilisateur : À chaque personne, peuvent être associés des comptes d'accès aux différents systèmes et applications. Le compte contient des données qui permettent d'y accéder (identifiant + mot de passe).
Compte générique : Compte anonyme n'appartenant pas à une personne en particulier. Il peut être employé par plusieurs utilisateurs (exemples : « Admin », « User1 »).
Droits d'accès : Allocation à un utilisateur de droits pour accéder à une ressource du système d'information.
Authentification forte : une authentification forte (ou multi-facteurs) nécessite deux facteurs d'authentification dont :

- ✓ Quelque chose que l'utilisateur connaît (mot de passe, code PIN, etc.)
- ✓ Quelque chose que l'utilisateur possède (carte à puce, jeton USB, carte magnétique, RFID, un téléphone pour recevoir un code SMS, etc.)
- ✓ Quelque chose que l'utilisateur est (biométrie, empreinte, etc.)

Règles de gestion:

- Le présent document ne remplace pas la documentation de gouvernance en matière de gestion des accès logiques de chaque établissement.
- Les bonnes pratiques recommandées par ce document peuvent être adaptées et alignées aux politiques internes de chaque établissement.
- Les établissements du réseau peuvent bénéficier du présent document pour bonifier leur processus de gestion des accès.

Description de l'instruction

Le COCD invite les établissements à considérer les bonnes pratiques et recommandations communiquées par la présente instruction en matière de gestion des comptes sensibles. Ces recommandations consistent principalement à appliquer le principe de moindre privilège, adopter une politique de gestion de mots de passe et d'authentification et mettre en place une procédure de gestion et de revue des accès.

Principe de moindre privilège:

Le principe de moindre privilège doit être appliqué. Cela implique l'attribution des privilèges et droits d'accès qui sont strictement nécessaires pour les activités associées à chaque personne. À titre d'exemple, un utilisateur n'a pas besoin d'un compte administrateur sur sa machine pour effectuer son travail quotidien.

Réduisez au maximum le nombre d'utilisateurs ayant des privilèges d'administrateur ou ayant accès à des données sensibles et revalidez souvent le besoin d'accès privilégié pour ces utilisateurs. Les comptes à hauts privilèges ne doivent être utilisés que dans des conditions bien précises et par des personnes identifiées et légitimes.

Gestion de mots de passe et authentification:

Les mots de passe des comptes ordinaires, des comptes administratifs et des comptes de services, doivent être gérés conformément à une politique de gestion de mots de passe établie auparavant.

La politique de gestion de mots de passe doit définir la taille minimale d'un mot de passe, sa complexité (catégories de caractères exigés) ainsi que d'autres conditions pour les mots de passe acceptés. La sécurité la plus forte doit être appliquée aux comptes ayant le plus de privilèges et dont l'accès frauduleux aurait le plus d'impact.

Le partage et le stockage en clair des mots de passe doit être interdit. L'utilisation d'une solution spécialisée pour la gestion des mots de passe ainsi qu'un coffre-fort de mots de passe labellisé est recommandée pour éviter de stocker en clair des mots de passe sur les postes d'administration. L'accès à ce coffre-fort doit être limité aux personnes légitimes dont l'accès est justifié et identifié.

Privilégiez lorsque c'est possible une authentification forte pour accéder à des applications sensibles ou pour les accès à distance au réseau.

Il est également recommandé de limiter le nombre de tentatives d'authentification et de particulièrement faire attention à monitorer toute tentative d'accès répétée ou présentant un caractère inhabituel à des comptes sensibles.

Comptes génériques et comptes par défaut:

Afin de faciliter l'attribution d'une action sur le système d'information en cas d'incident ou d'identifier d'éventuels comptes compromis, les comptes d'accès doivent être nominatifs. Identifiez nommément chaque personne accédant au système et distinguez les rôles utilisateur/administrateur.

Un compte unique et nominatif est requis pour chaque accès octroyé. Les comptes génériques sont à éviter, à moins d'en justifier techniquement l'utilisation.

Les comptes d'administration par défaut ne doivent pas être utilisés pour les tâches courantes d'administration. Ils ne doivent être connus que par un nombre très restreint de personnes. Des comptes nominatifs sont attribués à chaque administrateur.

Gestion des comptes à hauts privilèges :

Les comptes d'administration ne doivent pas être utilisés pour ouvrir des sessions de travail sur des postes autres que ceux réservés aux tâches d'administration. Cette recommandation revêt un caractère d'autant plus critique si les postes administrés ont accès à Internet. Les recommandations suivantes peuvent être émises :

- Effectuez les tâches administratives à partir d'un poste de travail particulier qui n'est pas connecté à Internet ou qui est dépourvu d'un courriel à accès libre.
- Les accès ayant des droits privilégiés doivent être identifiés et documentés pour chacune des composantes du système d'information (applications, bases de données, systèmes d'exploitation, composants informatiques, documents, etc.). Les motifs d'attribution des privilèges d'accès de haut niveau doivent rester valides durant toute la période de leur attribution.
- Mettez en place une procédure formelle de révision des privilèges afin d'en assurer le maintien ou la révocation. Les comptes à hauts privilèges sont plus fréquemment révisés que les comptes ordinaires.

- Assurez-vous que l'accès en tant qu'administrateur réseau, administrateur système ou administrateur d'application est fait au moyen d'un compte utilisateur nominatif, distinct du compte utilisateur normal, et non générique afin de retracer les auteurs des actions effectuées et responsabiliser les intervenants.
- Assurez-vous que les postes de travail des administrateurs des réseaux, des administrateurs des systèmes ou des administrateurs d'applications se verrouillent automatiquement au-delà d'une courte période d'inactivité prédéterminée. Cette précaution permet de restreindre les risques d'une utilisation frauduleuse des privilèges de l'administrateur.
- Activez la journalisation pour assurer le suivi et le contrôle des activités réalisées par les comptes à hauts privilèges. Il doit être possible de dire qui a fait quoi et quand en cas de problème.

Revue des accès :

Comme indiqué précédemment, les comptes à hauts privilèges et ceux donnant accès à des données ou actifs sensibles doivent être référencés, cadrés par une politique regroupant les principes énoncés plus tôt et leur existence révisée à intervalle régulier.

Pour être efficace et pérenne, ceci devrait s'inclure dans un processus plus global de gestion et de revue des accès. Ce processus, avant tout de gouvernance, aura comme résultat une cartographie des utilisateurs et de leurs comptes associés, les accès que cela implique en fonction des rôles et responsabilités de chacun et donc, les risques associés et la détection d'anomalies. Il est recommandé d'automatiser le plus possible la mise à jour de cette cartographie en l'adossant notamment aux processus des ressources humaines et en mettant en place des moyens techniques permettant l'exécution facile de revues formalisées.

Avant de lancer la mise en place d'un programme complet qui peut être complexe et coûteux, il est important de garder à l'esprit que les processus de revue nécessitent un plan, mais n'ont pas à être immédiatement lourds et complexes, surtout si aucun autre de ce type n'est déjà en place. Afin d'avoir des résultats rapides, des revues simples et de complexité progressive au fil des itérations sont préférables à des processus complexes à maintenir et dont les observations sont longues à obtenir. Discernement et pragmatisme doivent aider l'organisme dans ses choix en fonction de son contexte.

Chaque revue sera l'occasion de relever les comptes non conformes à la politique mise en place (droits non justifiés, utilisateur ayant quitté l'organisation…) en se concentrant en priorité sur les comptes sensibles et identifier les mesures nécessaires à mettre en œuvre. Mesures dont l'efficacité sera vérifiée lors de l'itération suivante, qui permettra peut-être de détecter de nouvelles anomalies et d'ainsi mettre en place une démarche d'amélioration continue et de maitrise dans l'octroi des droits d'accès.

Les risques de fuite de données, acte malveillant, intrusions, mais aussi des impacts majeurs en cas de propagation de logiciels malveillants (comme des rançongiciels) seront ainsi limités.

N° : 2020-005.01
Date : 2020-10-29

Instruction relative à la protection contre les attaques par rançongiciels

CCCD

Instruction relative à la protection contre les attaques par rançongiciels

Objet de l'instruction

Remerciement:

Champ d'application

Définitions et terminologies

Contexte de l'instruction :

Au fil des années, ces attaques n'ont pas cesse de se développer pour devenir extrêmement sophistiquées, tant sur le plan technique que sur le plan organisationnel. C'est pourquoi les organisations sont appelées à prêter une attention particulière à la gestion du risque venant de ces menaces. Dans l'objectif de vous aider à faire face à cet ennemi extrêmement dangereux, nous avons élaboré cette instruction. Elle rappelle certaines bonnes pratiques qui s'avèrent efficaces pour réduire les risques d'attaques et les pertes en cas d'intrusion réussie.

Un cas récent dans les réseaux du MEQ/MES :

Un établissement de notre réseau a été victime d'une attaque par rançongiciel le 17 septembre 2020. Les données de plusieurs serveurs ont été encryptées par un maliciel qui demande de payer une rançon pour le déchiffrement. Dans l'éventualité que d'autres établissements du réseau soient ciblés par des attaques similaires, nous vous rappelons qu'il faut prendre les précautions nécessaires afin de protéger au mieux les données avant et après la survenance d'incidents pareils.

En termes de prévention :

Le niveau de sécurité d'une organisation est équivalent au niveau de sécurité de son maillon le plus faible. Cela dit, la protection contre les rançongiciel revient à améliorer la posture de sécurité globale de toute l'organisation. Pour ce faire, nous vous proposons les axes d'amélioration suivants :

- Mettre à jour régulièrement les applications ainsi que les systèmes d'exploitation clients et serveurs. Une priorité élevée devrait être attribuée aux systèmes les plus importants et ceux exposés à internet.
- Mettre à jour fréquemment les bases de signatures des systèmes de prévention d'intrusion et d'antivirus.
- S'assurer que les services d'antivirus et de détection et de préventions d'intrusion (IDS/IPS) sont activés sur les équipements de sécurité périmétrique.
- Appliquer une politique de filtrage des accès réseaux adaptée pour cloisonner les différentes zones réseaux notamment les postes de travail, les serveurs internes et les serveurs exposés à internet. Ainsi qu'une micro-segmentation des services au sein de chaque zone selon la sensibilité, l'usage et l'exposition aux risques.
- Contrôler et empêcher l'exposition de services sensibles sur internet et notamment ceux permettant l'administration à distance (RDP, SSH…).
- Mettre en place des solutions de filtrages des flux internet notamment le web, le DNS et la messagerie.
- Appliquer une politique de gestion des accès avec le principe du moindre privilège des utilisateurs et des applications. À cet effet, consultez l'instruction COCD - 2020-004.01.
- Utiliser l'authentification à plusieurs facteurs sur les systèmes qui la permettent.
- Procéder au durcissement des postes de travail, des serveurs et des solutions d'infrastructure réseau et sécurité; cela comprend toutes les configurations sécuritaires notamment l'installation d'antivirus, l'application des derniers correctifs, la réduction des composantes logicielles ou matérielles installées ainsi que les services activés au minimum requis par le métier.
- S'assurer que le processus de sauvegarde est fonctionnel. Des tests de restauration devraient être effectués pour valider le bon fonctionnement.
- Détenir une copie « hors-ligne » des sauvegardes critiques à intervalle régulier, étant donné que les données de sauvegarde peuvent également être ciblées par le rançongiciel.
- S'assurer que la journalisation des événements est activée au niveau des actifs importants notamment les coupe-feux, les solutions antivirales, les IPS/IDS et les serveurs. L'idéal est de les exporter vers une solution de gestion de logs centralisée permettant de surveiller en continu les événements de sécurité.
- Sécuriser les accès distants en utilisant des composantes à jour, des protocoles de chiffrement robustes et l'authentification à plusieurs facteurs.

- Vérifier régulièrement la présence d'indicateurs de compromission, notamment ceux fournis dans les bulletins de sécurité du COCD, au niveau de vos plateformes informatiques.
- S'assurer que la protection des pièces jointes est fonctionnelle au niveau des courriels.
- Sensibiliser les utilisateurs et les administrateurs par rapport au cyberrisque via des réunions d'informations, des quizz et des guides de bonnes pratiques.
- Mettre en œuvre un plan de réponse aux cyberattaques. Il convient d'envisager par exemple des canaux de communication de secours dans le cas d'interruption des services principaux de messagerie et de téléphonie et d'identifier les applications critiques à protéger et à faire repartir en priorité en cas d'incident.
- Mettre en place un comité de crise en matière en sécurité de l'information. Ce dernier sera fort utile si un événement survient.

En termes de réaction (lors d'une attaque) :

Ce qu'il ne faut pas faire :

- Paniquer, sachez que les attaquants vont essayer de vous pousser à payer la rançon.
- Payer la rançon, il n'y a aucune garantie que les données vont être déchiffrées ou restituées en cas d'exfiltration.
- Rétablir les services prématurément; cela peut permettre une relance de l'attaque.
- Éteindre ou redémarrer les machines affectées. Des malwares peuvent s'installer au niveau du noyau du système lors du redémarrage ce qui leur permet d'avoir plus de contrôle sur le système, facilitant ainsi la persistance et destruction des preuves.
- Démarrer les équipements éteints; cela peut provoquer la propagation du maliciel sur ces derniers.
- Utiliser des supports amovibles qui peuvent contaminer davantage de machines.

Ce qu'il faut faire:

Les étapes de cette phase requièrent des ressources spécialisées munies des bons outils afin de pouvoir comprendre ce qui s'est passé et rétablir les services graduellement en cas de préjudices majeurs, tout en assurant la protection des systèmes d'information le long du processus de gestion de l'incident. Si vous n'avez pas les ressources humaines suffisantes, il est recommandé de faire appel à des experts en matière de gestion des incidents pour vous accompagner. Dans le cas des incidents de rançongiciel avec faible impact, il serait judicieux de procéder, entre autres, aux actions suivantes :

- Isoler les équipements ou machines virtuelles infectés en les déconnectant du réseau le plus tôt possible et couper toute connexion depuis et vers internet.
- Mettre les machines infectées en veille prolongée pour suspendre les éventuels chiffrements en cours tout en préservant les données de la mémoire dynamique qui peuvent contenir des informations utiles pour les investigations et le déchiffrement.
- Contacter le COCD le plus tôt possible afin que nous puissions mieux vous aider.
- Mettre en place ou activer le comité de gestion de crise interne.
- Contacter votre assureur si vous avez déjà souscrit à une assurance cyber pour une assistance juridique et une couverture financière du préjudice matériel et immatériel.
- En cas de manque de ressources : appeler une assistance technique.

- Protéger les sauvegardes qui peuvent être l'unique solution pour récupérer certaines données.
- Réinitialiser les mots de passe des comptes à privilèges et des comptes compromis.
- Préserver les preuves : éviter toutes destruction/reformatage ou effacement. Quelquefois les données peuvent être déchiffrées s'il existe un outil qui le permet. Elles constituent aussi un artefact pour une enquête approfondie par les spécialistes et une preuve dans les enquêtes policières.
- Prendre des points de contrôle (snapshots) dans le cas d'infection de machines virtuelles.
- Consulter un spécialiste des fuites (Breach Coach) pour déterminer les actions légales à entreprendre.
- Exporter les logs des équipements réseaux et solutions de sécurité (IPS, Filtre web).
- Restaurer les données depuis les sauvegardes effectuées sur des machines nouvellement installées, tout en vérifiant que les sauvegardes sont saines.
- Garder un journal écrit de tous les événements et actions liés à l'incident, en mentionnant la date, l'heure, le nom de la personne qui a fait l'action ou qui a informé sur l'événement et une description.

Pour comprendre ce qui s'est passé :

- Mise en quarantaine des équipements ou machines virtuelles suspects.
- Analyse complète des systèmes suspects par un antivirus et un antimaliciel.
- Analyse du trafic sur les coupe-feux pour vérifier la présence d'activité suspicieuse.
- Analyse des événements sur les solutions de sécurité comme l'antivirus ou l'IPS/IDS.
- Analyse des données des machines infectées pour déterminer s'il y a des événements liés à l'incident.
- Analyse du volume des données transitant par le réseau pour détecter toute exfiltration des données.

Québec

N° : 2020-006.01
Date : 2020-12-18

Instruction relative aux échanges sécurisés avec le COCD

COCD

Instruction relative aux échanges sécurisés avec le COCD

Objet de l'instruction

L'objectif de cette instruction est de fournir aux correspondants des établissements des réseaux de l'éducation un ensemble de consignes et de bonnes pratiques permettant l'échange d'informations de manière sécurisée entre les organisations des réseaux de l'éducation et le COCD de l'Éducation.

Champ d'application

- Les correspondants du COCD du ministère de l'Éducation et du ministère de l'Enseignement supérieur
- Les correspondants du COCD dans tous les organismes des réseaux de l'éducation

Définitions et terminologies

Données sensibles : Toute information dont la nature ou la signification induirait, si leur diffusion était inappropriée, un impact financier, légal, stratégique, en termes de réputation et/ou au niveau des critères de sécurité pour les actifs concernés (en facilitant la conduite d'actions malveillantes par exemple).

Niveaux de confidentialités : Le COCD distingue 4 niveaux de confidentialité des données qui définissent les modalités de leur diffusion :

- Privé : Données très sensibles à ne transmettre qu'aux individus directement concernés par les informations ou légitimes dans le droit d'en prendre connaissance (souvent ce sera le CSGI). Elles ne peuvent être retransmises par les destinataires.
- Diffusion restreinte : Données sensibles à ne diffuser que de façon limitée au sein de l'organisation, vers des équipes clairement identifiées. Pas de diffusion ouverte sur des plateformes de communication. La rediffusion nécessite un accord des propriétaires.
- Diffusion interne : Données non publiques mais diffusables largement dans une ou plusieurs organisations/communautés.
- Public : Aucune restriction, données publiques.

OpenPGP : Standard défini dans la RFC 4880 servant notamment pour le chiffrement et l'authentification des courriels électroniques.

GPG/GnuPG : Gnu Privacy Guard est l'implémentation Gnu du standard OpenPGP.

Règles de gestion:

- Ce document s'adresse en priorité aux correspondants du COCD de l'Éducation pour une application à leur niveau. Il se concentre sur les outils utilisés dans le cadre du COCD.
- Le présent document définit les règles de protection de la donnée à mettre en place pour les communications avec le COCD dans le cadre de ses services entre les différents correspondants sécurité.
- Il a également pour but de conseiller plus globalement l'utilisation de protections pour les communications d'informations sensibles au sein des réseaux de l'éducation (sans toutefois conseiller une solution technique en particulier).
- Il vient en complément des politiques et solutions déjà existantes. Si certaines parties sont déjà couvertes par des solutions existantes (Microsoft 365, solutions de chiffrements, etc.), il convient d'en informer le COCD pour adapter les processus de son côté, mais pas de remplacer ce qui est en place.
- Cette instruction est liée au document détaillant les canaux de communication du COCD et leurs niveaux de confidentialité (les détails d'utilisation des outils y sont présents).

Description de l'instruction

Dès lors que les données échangées ont un caractère sensible, il est essentiel de les protéger afin de garantir leur confidentialité, leur authenticité et leur intégrité pour ainsi éviter des impacts négatifs pour les entités auxquelles elles appartiennent.

Il est communément admis que des moyens d'échanges d'informations comme le courriel ne sont pas adaptés pour l'envoi ou la réception de données confidentielles. En effet, ces informations sont par défaut lisibles et la sécurité des réseaux et serveurs traversés par un message ne peut être garantie de bout en bout. Le risque d'interception ou de divulgation de l'information n'est donc pas négligeable y compris lorsque des données sont au repos sur le poste de travail ou l'espace en ligne.

L'utilisation des canaux de communication peut également constituer un enjeu lorsque l'information est diffusée dans des groupes larges et stockée sans contrôle ni protection.

Les moyens de palier à cela sont notamment l'utilisation de moyens de chiffrement permettant de rendre les données inaccessibles et l'application de bonnes pratiques et de discernement dans le partage de ces données.

Plusieurs cas de figure vont être décrits par la suite avec des conseils et des bonnes pratiques. Les parties suivantes sont également à prendre de façon plus générique dans le cadre de la protection des données.

Pour toute situation, il convient de garder à l'esprit que le meilleur outil que nous pourrions suggérer est avant tout votre propre jugement. Il est important de se poser les bonnes questions avant de partager une information afin de faire les bons choix : Ces informations sont-elles sensibles? Que se passerait-il si les mauvaises personnes venaient à les lire? Les personnes à qui je les diffuse ont-elles vraiment le droit/la nécessité d'en prendre connaissance dans le cadre de leur fonction? Si je stocke ces fichiers, quelqu'un peut-il y accéder?

D'un point de vue technique, plusieurs outils/fonctions et bonnes pratiques peuvent venir renforcer nos cas d'utilisations et apporter une protection optimale. Ils sont notamment activables via les plateformes infonuagiques souvent utilisées comme point central des échanges (comme Azure) :

- Une authentification multifacteur aux outils permettant l'accès et l'échange de la donnée (p. ex. Teams, Outlook)
- Marquer les données et les contrôler via des politiques (p. ex. Azure Information Protection)
- Empêcher les téléchargements sur des équipements non contrôlés (p. ex. Microsoft Cloud App Security)
- Prévoir un espace de partage contrôlé et sécurisé permettant de maitriser les accès, la rétention et les téléchargements des fichiers partagés
- Chiffrement des disques des postes de travail (en priorité les machines traitant de la donnée sensible) (p. ex. BitLocker)

(À noter que chaque activation de fonctionnalité doit faire l'objet d'un projet de qualification et de tests avant généralisation.)

Envoi de données par courriel

Niveau de confidentialité maximale sans chiffrement	Diffusion interne
Niveau de confidentialité maximale avec chiffrement	Privé
Moyen conseillé	OpenPGP/GnuPG s/MIME Chiffrement de messages dans Microsoft 365 Mailvelope

Le courriel est le mode de communication le plus utilisé en entreprise et de nombreuses données sensibles sont échangées sans protection. Il est une source de fuite de données classique notamment en cas d'accès non autorisé.

Les données échangées dans le cadre des communications sur les incidents peuvent avoir une nature sensible, car elles révèlent des détails sur ces incidents ou des informations stratégiques dont la diffusion publique peut avoir des impacts médiatiques ou permettre la conduite d'attaques opportunistes.

Outre le contrôle des destinataires, il est fortement conseillé de protéger les courriels contenant des données sensibles (et obligatoire pour des données de niveau privé) au moyen de chiffrement. OpenPGP/GnuPG est utilisé par le COCD, il nécessite l'installation de logiciels tiers, la création de paires de clés de chiffrement et l'échange de clés publiques entre les correspondants.

Outils conseillés

- Client Outlook: Gpg4win (Gnu Privacy Guard, Kleopatra, GpgEx et GpgOL)

Plusieurs logiciels existent pour permettre l'utilisation de OpenPGP/GnuPG sous Windows. Le COCD conseille Gpg4win pour une utilisation gratuite avec Outlook et GpgOL.

- Courriel web : Mailvelope

  Si le courriel web est utilisé régulièrement pour l'envoi de messages sensibles (et qu'aucune solution n'est déjà proposée), il est conseillé de prévoir un moyen de protection pour ce canal. Le COCD conseille Mailvelope pour une utilisation gratuite et facile avec un navigateur web.

- Gestionnaire de mots de passe (KeePass, Password Safe, LastPass, 1Password, etc.)

Envoi de données par Teams

Niveau de confidentialité maximale sans chiffrement	Diffusion interne (canaux de groupe)
Niveau de confidentialité maximale avec chiffrement	Privé
Moyen conseillé	OpenPGP/GnuPG

Les données traitées par Teams sont chiffrées en transit et au repos cependant les canaux de communications offerts ne protègent pas des accès non autorisés. En effet, ils peuvent comprendre un grand nombre de correspondants dont le droit à prendre connaissance de certaines informations sensibles ne peut être vérifié.

Dans ce contexte, il convient de rester vigilant à ce qui est partagé, comment cela est partagé, ainsi que de contrôler qui a accès à quoi (notamment au niveau SharePoint). Les contrôles et revues des accès ainsi que la sensibilisation seront des mesures adéquates dans ces cas.

Lorsque les informations deviennent sensibles, il est préférable de privilégier les communications en direct, en groupe restreint ou appels et de n'échanger que les informations nécessaires. Dans le cas d'informations de niveau privé, il est alors indispensable de chiffrer les fichiers échangés (l'option d'un espace de partage séparé, contrôlé et sécurisé, peut être également envisagée en protection supplémentaire).

À noter que tout fichier sensible devrait être stocké sous forme chiffrée.

Outils conseillés

- Chiffrement de fichier: Gpg4win (Gnu Privacy Guard, Kleopatra, GpgEx et GpgOL)

Plusieurs logiciels existent pour permettre l'utilisation de OpenPGP/GnuPG sous Windows. Le COCD conseille Gpg4win pour une utilisation gratuite avec Kleopatra et GpgEx permettant de chiffrer et déchiffrer des fichiers.

- Gestionnaire de mots de passe (KeePass, Password Safe, LastPass, 1Password, etc.)

Stockage de fichiers

Niveau de confidentialité maximale sans chiffrement	Diffusion interne
Niveau de confidentialité maximale avec chiffrement	Privé
Moyens conseillés	OpenPGP/GnuPG Options natives des systèmes ou applications

Comme indiqué précédemment, une information sensible devrait être protégée au moment de son transit, mais elle doit l'être également au repos de façon à la protéger des accès non légitimes et des vols.

Par principe, il n'est pas recommandé de stocker des fichiers sensibles sur les postes de travail ou appareils mobiles et encore moins de manière non protégée.

Si les fichiers sensibles doivent être stockés, ils peuvent être également protégés individuellement au moyen de conteneurs de chiffrement ou d'outils simples d'utilisation permettant un chiffrement asymétrique ou symétrique.

Outils conseillés

- Chiffrement de fichier: Gpg4win (Gnu Privacy Guard, Kleopatra, GpgEx et GpgOL)

  Le COCD conseille Gpg4win pour une utilisation gratuite avec Kleopatra et GpgEx permettant de chiffrer et déchiffrer des fichiers y compris de manière symétrique avec un seul mot de passe de déchiffrement partagé (dans ce cas, prévoir une complexité suffisante et le transmettre aux correspondants via un canal séparé).

- Gestionnaire de mots de passe (KeePass, Password Safe, LastPass, 1Password, etc.)

N° : 2021-007.01
Date : 2021-01-11

Instruction relative à la journalisation des évènements

Instruction relative à la journalisation des évènements

Objet de l'instruction

La présente instruction décrit les bonnes pratiques en termes d'organisation d'une stratégie de journalisation et donne des pistes concernant des évènements pertinents à journaliser.

Champ d'application

- Le MES/MEQ
- Tous les établissements des réseaux de l'éducation

Définitions et terminologies

- **Évènement :** Une occurrence observable au niveau d'un système, d'une application ou du réseau.
- **Journal d'évènements :** Composant ou fichier permettant de tracer les évènements ayant eu lieu au niveau d'un actif.
- **Journalisation :** La journalisation est l'enregistrement et le stockage des évènements affectant une application, machines, processus ou tout autre actif. Ceci permet notamment de retracer une activité dans le temps.
- **Données sensibles :** Toute information dont la nature ou la signification induirait, si leur diffusion était inappropriée, un impact financier, légal, stratégique, en termes de réputation et/ou au niveau des critères de sécurité pour les actifs concernés (en facilitant la conduite d'actions malveillantes par exemple).
- **EDR (Endpoint Detection and Response):** Catégorie de solutions ou d'outils permettant la détection et le blocage d'activités ou de comportements suspects et de menaces avancées au niveau des hôtes. Ils permettent également d'organiser une investigation en profondeur et une réponse face aux détections directement au niveau de ces hôtes.
- **SIEM (Security Information and Event Management):** Système ou architecture de systèmes permettant la collecte, le stockage, la normalisation et l'interprétation de données dont la fonction principale est d'accélérer, voire d'automatiser, la détection et l'analyse d'évènements de sécurité à de grandes échelles et de manière centralisée. À ne pas confondre avec un « simple » outil de gestion des journaux qui est un sous-ensemble et qui n'apportera pas la corrélation et la détection temps réel des menaces de sécurité.

Règles de gestion:

- Ce document vient en complément des politiques de journalisation déjà en place et a pour but de les bonifier.
- Il vise notamment à faciliter les phases d'investigations post-incident et préparer les mises en place de systèmes de détections temps réel pour les évènements de sécurité.
- Il se concentre uniquement sur les journaux apportant une plus-value sécurité.
- Étant donné le grand nombre d'équipements, d'applications et de contextes différents, il n'est pas possible de donner des consignes précises. Pour cette raison, ce document restera générique et apportera plutôt des pistes de réflexion ainsi que des bonnes pratiques pour les administrateurs.
- Les évènements cités pour Windows sont des évènements minimaux à activer conformément aux bonnes pratiques et recommandations de l'éditeur. Il faut prendre ces éléments comme une base et activer d'autres évènements en fonction des besoins et du contexte de chaque organisation (impossible à traiter ici).
- Les activations de nouveaux journaux doivent toujours se faire après une étude validant les capacités de stockage, de charge et les licences nécessaires pour l'activation et/ou la collecte de ces derniers.

- Les aspects légaux et de protection des données personnelles liés à la journalisation ne seront pas abordés.
- Ce document est amené à évoluer et à être enrichi progressivement.

Introduction:

Il est dans les bonnes pratiques pour tout système d'information de cadrer et formaliser un processus de gestion des journaux des applications et équipements, notamment pour les journaux de sécurité. Ces derniers sont une source indispensable d'informations pour :

- Investiguer et analyser les incidents en cours ou passé.
- Détecter un incident de sécurité et permettre une réaction adéquate pour limiter ses impacts.
- Dans certains cas, répondre à des obligations légales.
- Apporter une preuve de mise en place ou de fonctionnement à des contrôles de sécurité.

Une mauvaise gestion des journaux et/ou la non-activation de journaux utiles peuvent donc avoir des conséquences graves.

À noter que la mise en place d'une politique de gestion des journaux est un prérequis à tout projet SIEM, mais cela n'empêche pas de la mettre en place en plusieurs étapes. Une journalisation bien définie et maitrisée est une base solide pour le fonctionnement efficace de toute détection d'incidents.

Prérequis:

Afin de pouvoir être efficace, la stratégie de journalisation doit reposer sur certains prérequis importants permettant de déterminer quels logs et quels évènements sont utiles:

- Un inventaire des actifs afin d'identifier leur importance et leur capacité de journalisation.
- Une étude de contexte voire de risques afin d'identifier l'exposition aux menaces, leur nature et impact potentiel et donc les besoins en journalisation pour tracer et détecter les évènements liés.
- Une gestion des identités et des accès (GIA). Ceci permet de déterminer le contexte et les besoins afin de tracer les accès aux ressources et répondre à la question : Qui accède à quoi et depuis où? Et être ainsi capable de détecter les évènements anormaux. C'est une activité centrale dans un système d'informations.

Comme tout projet à caractère complexe, il est recommandé de commencer de façon simple et pragmatique et d'améliorer progressivement la stratégie par itérations successives.

À cela, nous pouvons ajouter des prérequis techniques pour les journaux eux-mêmes:

- Le format des journaux doit être lisible, structuré et ingérable par des outils tiers (Syslog, JSON, CEF, Windows event, ELF, etc.).
- Les journaux doivent pouvoir être exportables ou requêtables facilement.
- Les journaux doivent être horodatés et l'heure des équipements synchronisée sur des serveurs de temps fiables.

En résumé, les données doivent permettre de savoir quels évènements ont eu lieu, qui ou quoi les a causés, quand et comment. À cet effet, plusieurs journaux devront donc être activés ou à configurer pour enregistrer les informations utiles.

Une bonne journalisation repose également sur une bonne configuration des équipements, machines, applications et sur une revue régulière de ces configurations. Ceci est particulièrement vrai pour les

équipements de sécurité et leurs stratégies de détection/blocage (ainsi que leur journalisation), qui doivent être contrôlés régulièrement pour rester efficaces.

Bonnes pratiques

Collecte de logs

Dépendant de la stratégie adoptée, il est en général vivement recommandé d'organiser une collecte centralisée des journaux d'évènements. Cela facilite leurs gestion, exploitation et sauvegarde. Un temps précieux peut être gagné en cas d'investigation via cette méthode. Plusieurs outils et de nombreuses solutions permettent de facilement mettre en place une telle centralisation.

En fonction des organisations et de la complexité du système d'informations, il peut être pertinent d'avoir une architecture distribuée et une redondance des serveurs de collecte de façon à éviter les pertes et optimiser les charges. Ceci doit être particulièrement envisagé en cas de grande volumétrie de journaux et de typologie favorisant les goulots d'étranglement. La fluidité des échanges de journaux et les performances réseautiques globales du système d'information doivent être préservées en tout temps.

Rotation

Les journaux ne peuvent être conservés indéfiniment au même emplacement et dans les mêmes fichiers. Ils doivent donc suivre une politique de rotation suivie d'une compression, voire d'un archivage, permettant d'étendre la rétention tout en maitrisant la charge et les besoins en stockage.

Cette rotation peut être basée sur des critères temporels et/ou de taille, le choix et le seuil vont dépendre du contexte de chaque organisme. Des considérations légales, réglementaires, de licence ou de moyens techniques disponibles sont à prendre en compte.

De manière générale, il est conseillé de conserver au minimum 6 mois de journaux.

Verbosité

Certains journaux peuvent avoir des niveaux variables et configurables de verbosité. Les informations fournies à certains niveaux peuvent donc être plus détaillées et apporter des éclaircissements différents sur certaines situations.

Malheureusement, la verbosité est à ajuster en fonction du contexte et des équipements et il est difficile de pouvoir conseiller efficacement quelque chose de standard. Les administrateurs doivent donc tester quel niveau est le plus approprié pour apporter les bonnes informations dans la plupart des situations.

À noter que la logique du « plus grande est la verbosité mieux c'est » est contrebalancée par les limitations en stockage, performances et parfois licences à considérer lorsque l'on configure ce paramètre. Généralement, il n'est donc pas recommandé d'utiliser des niveaux de verbosité élevés comme « debug », « information » ou même « notification » sur de longues périodes sans une véritable justification.

Protection

Les journaux d'évènements sont des éléments sensibles qu'il convient de préserver pour :

- Préserver les informations utiles des fichiers et éviter les modifications intentionnelles ou non.
- Éviter leurs accès non autorisés car ils peuvent potentiellement contenir des informations sensibles.

Les recommandations suivantes sont très fortement conseillées:

- Restreindre l'accès aux logs à quelques comptes ayant le droit en lecture.
- Si une collecte est effectuée, elle doit être effectuée par des comptes avec peu de privilèges.
- Dans le cas d'une collecte centralisée, il est recommandé de placer les serveurs de collecte dans une zone d'administration ou séparés des périmètres utilisateurs et internet.
- Dans des contextes réglementaires spécifiques, il peut être pertinent d'envisager l'utilisation de moyens de chiffrement et de contrôle d'intégrité.
- Si le transfert de journaux s'effectue sur un réseau non maitrisé, il est recommandé d'utiliser un canal chiffré.

Les évènements à activer :

Il est important de noter que toute activation repose avant tout sur un contexte et que d'autres évènements que ceux conseillés peuvent être parfois pertinents. Cette réflexion basée sur les besoins en journalisation permettra également de déterminer le niveau de verbosité nécessaire.

Les sources de logs à ne surtout pas négliger sont les suivantes:

- Serveurs et postes de travail
- Applications (p. ex., application web, base de données, etc.)
- Outils de sécurité (p. ex., antivirus, IDS/IPS, EDR, etc.)
- Infrastructures et passerelles (p. ex., pare-feu, proxy, active directory, DNS, bastion, etc.)

De façon classique sur les applications et machines, les types d'évènements suivants sont recherchés :

Type	Exemple
Authentification	- Réussites et échecs d'authentification
Gestion des comptes et des droits	- Ajouts/suppressions/modification de comptes/groupes/rôles - Affectations/suppressions de droits aux comptes/groupes/rôles - Modification de mot de passe
Accès aux ressources	- Accès ou tentatives d'accès en lecture/écriture/exécution aux ressources - Les accès à des ressources ou données sensibles doivent notamment être tracés et surveillés.
Modification des stratégies de sécurité	- Éditions, applications, réinitialisations de configurations
Activité des processus	- Démarrages/arrêts - Dysfonctionnements - Chargements/déchargements de modules
Activité des systèmes	- Démarrages/arrêts - Dysfonctionnements/surcharges du système - Chargements/déchargements de modules - Activité matérielle (défaillances, connexions/déconnexions physiques, etc.)

Journaux de sécurité	Tout évènement de détection d'activité suspecte générée par l'application. Les systèmes et applications peuvent parfois détecter automatiquement des actions suspectes et tracer cela dans les journaux. Il est important de les considérer.
Accès administrateur	Tout accès et actions détaillées effectués avec un compte administrateur. Il est important que les actions effectuées avec des comptes disposant de droits étendus soient rigoureusement tracées et surveillées.

Pour les équipements réseaux, nous pouvons ajouter ces types d'évènements supplémentaires:

Type	Exemple
Trafic autorisé et bloqué	Toute requête aussi bien autorisée que bloquée avec au minimum: source et destination (NAT aussi), protocole, statut, ports source et destination (NAT aussi), interfaces d'entrée et de sorties, flag, action, nom de machine, octets envoyés et reçus, utilisateur source et destination, nom de règle, réseau virtuel, session id, nom d'application, niveau de criticité des évènements.
Journaux de sécurité	Tout journal sécurité permettant de savoir si une menace est détectée et/ou bloquée avec au minimum: source et destination (NAT aussi), protocole, statut, ports source et destination (NAT aussi), interfaces d'entrée et de sorties, signature, action, action par défaut, utilisateur, nom de machine, règle, périmètre, niveau de criticité des évènements.
Journaux système	Authentifications sur l'équipement, modifications de configurations, activités VPN, performances, lignes de commandes exécutées.

À noter qu'en fonction des options activées il peut être indispensable de penser à l'activation de journaux spécifiques supplémentaires (DLP, IPS, antivirus, etc.). Les administrateurs sont invités à lister les modules utiles et à déterminer lesquels ont une valeur pour la surveillance/détection.

Pour les serveurs web, les éléments suivants sont à activer dans les logs :

Type	Exemple
Journaux d'accès	Détail des requêtes, méthodes, ressources, code de retour, referer, user-agent, taille des objets retournés, ip source, utilisateur du client.

Journaux d'erreurs	Source intéressante d'information. Le niveau de log à utiliser pour avoir les bonnes informations va dépendre de la solution utilisée, du contexte et des moyens de stockage. P. ex., pour Apache le niveau « warn » peut-être suffisant dans la plupart des cas.

Évènement Windows

Dans les environnements Windows, il est recommandé d'activer les politiques d'audit suivantes afin d'aider à la détection de comportements suspects :

Pour rappel, ces éléments sont des recommandations, les administrateurs doivent valider leurs activations en fonction de leur contexte et procéder à des tests avant passage à la production.

Pour Windows 10, Windows 8, Windows 7 :

	De base		Pour périmètres critiques	
Politique d'audit	**Success**	**Failure**	**Success**	**Failure**
Account Logon				
Audit Credential Validation	x		x	x
Audit Kerberos Authentication Service			x	x
Audit Kerberos Service Ticket Operations			x	x
Audit Other Account Logon Events			x	x
Account Management				
Audit Computer Account Management	x		x	x
Audit Other Account Management Events	x		x	x
Audit Security Group Management	x		x	x
Audit User Account Management	x		x	x
Detailed Tracking				
Audit DPAPI Activity			x	x
Audit Process Creation	x		x	x
Logon and Logoff				
Audit Account Lockout			x	
Audit Logoff	x		x	
Audit Logon	x	x	x	x
Audit Special Logon	x		x	x
Policy Change				
Audit Audit Policy Change	x	x	x	x
Audit Authentication Policy Change	x		x	x
System				
Audit IPsec Driver	x	x	x	x

Audit Security State Change	x	x	x	x
Audit Security System Extension	x	x	x	x
Audit System Integrity	x	x	x	x

Pour Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows 2008:

	De base		Pour périmètres critiques	
Politique d'audit	**Success**	**Failure**	**Success**	**Failure**
Account Logon				
Audit Credential Validation	x	x	x	x
Audit Kerberos Authentication Service			x	x
Audit Kerberos Service Ticket Operations			x	x
Audit Other Account Logon Events			x	x
Account Management				
Account Computer Account Management	x	x (sur DC)	x	x
Audit Other Account Management Events	x	x	x	x
Audit Security Group Management	x	x	x	x
Audit User Account Management	x	x	x	x
Detailed Tracking				
Audit DPAPI Activity			x	x
Audit Process Creation	x		x	x
DS Access				
Audit Directory Service Access	x (sur DC)	x (sur DC)	x (sur DC)	x (sur DC)
Audit Directory Service Changes	x (sur DC)	x (sur DC)	x (sur DC)	x (sur DC)
Logon and Logoff				
Audit Account Lockout			x	
Audit Logoff	x		x	
Audit Logon	x	x	x	x
Audit Other Logon/Logoff Events			x	x
Audit Special Logon	x		x	x
Policy Change				
Audit Audit Policy Change	x	x	x	x
Audit Authentication Policy Change	x		x	x
System				
Audit IPsec Driver	x	x	x	x
Audit Security State Change	x	x	x	x
Audit Security System Extension	x	x	x	x
Audit System Integrity	x	x	x	x

Dans le cadre d'une surveillance organisée, les évènements de sécurité suivants sont à monitorer au minimum:

1102, 4624, 4625, 4648, 4657, 4663, 4688, 4700, 4702, 4719, 4720, 4722, 4723, 4724, 4727, 4728, 4732, 4735, 4737, 4739, 4740, 4754, 4755, 4756, 4767, 4799, 4825, 4946, 4948, 4956, 5024, 5033, 8001, 8002, 8003, 8004, 8005, 8006, 8007, 8222

Si ces évènements ne sont pas activés, il convient d'étudier cette possibilité.

À noter que certains évènements ne seront pas disponibles sur des systèmes plus anciens que Windows 2016 et 10. Il est important de toujours disposer de versions système récentes et supportées.

Comme précisé précédemment, des besoins et contextes spécifiques peuvent nécessiter l'activation d'autres évènements. Chaque organisme est invité à se pencher sur cette question.

Pour aller plus loin

Voici une liste de ressources permettant d'apporter plus de détails sur ces sujets importants et complexes :

https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

https://apps.nsa.gov/iaarchive/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/security-configuration/applications/assets/public/upload/Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf&WpKes=aF6woL7fQp3dJiZsWp9tuYzewswdCagWY2vG6J

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltd346db979178897d/5e9dfdd5dac81811514a1b08/information_logging_standard.pdf

Québec

N° : 2021-008.01
Date : 2021-03-15

Protection des domaines de courriels

COCD

Instruction relative à la protection des domaines de courriels

Objet de l'instruction

L'objectif de cette instruction est de fournir aux organismes de l'Éducation les bonnes pratiques et méthodes afin de protéger leurs noms de domaines de courriels et ainsi réduire le risque d'usurpation et d'hameçonnage pour les organismes et leurs correspondants. Les protections proposées dans ce document seront « Sender Policy Framework » (SPF), « Domain-based Message Authentification, Reporting and Conformance » (DMARC) et « DomainKeys Identified Mail » (DKIM) ainsi que leur méthode de déploiement et nos recommandations.

Champ d'application

- Tous les organismes des réseaux de l'Éducation et de l'Enseignement supérieur

Définitions et terminologies

Hameçonnage: Type d'attaque basée sur des techniques d'ingénierie sociale afin de tromper les utilisateurs en leur faisant croire à la légitimité notamment d'un courriel afin de soutirer des informations sensibles (personnelles, bancaires, NAS, etc.) ou permettre la propagation de logiciels malveillants via des pièces jointes ou liens.

Règles de gestion:

- Le présent document définit les méthodes de protection de domaines de courriels à mettre en place pour réduire l'impact d'une usurpation. Il est fortement conseillé de procéder à une étude et à des tests préliminaires avant toute mise en place.
- Les protections présentées ici sont des propositions. Il convient pour chaque organisme d'élaborer son plan de protection.
- Cette instruction va se concentrer essentiellement sur les environnements Microsoft cependant des équivalents sont également disponibles pour d'autres fournisseurs de services.

Description de l'instruction

L'hameçonnage est un des vecteurs principaux de problèmes de sécurité dans le domaine de l'éducation. Il est source de vol d'informations personnelles et confidentielles ainsi que de propagation de logiciels malveillants dont certains avec un impact majeur comme les rançongiciels.

Ces attaques se basant la plupart du temps sur l'usurpation de domaines légitimes afin de tromper les utilisateurs, il convient de limiter les moyens offerts aux attaquants en déployant des mécanismes au niveau des infrastructures de courriels elles-mêmes de manière à faciliter la détection et le blocage des menaces ainsi que préserver la réputation ces domaines.

Trois protocoles permettent d'adresser cette problématique : SPF, DKIM et DMARC.

Ces protocoles vont permettre de :

- Perturber la distribution de messages malveillants;
- Réduire le risque de réussite d'une campagne d'hameçonnage;
- Préserver la réputation d'un domaine utilisé pour l'envoi de courriels;
- Identifier et bloquer plus facilement des messages malveillants;
- Améliorer globalement la sécurité des organismes.

Leurs bénéfices au niveau global dépendant principalement de leur prise en compte chez les expéditeurs ainsi que chez récepteurs, et sachant que leur activation n'est pas généralisée, cette instruction vise à transmettre

cette bonne pratique pour observer des effets en premier lieu au niveau des domaines concernés dans l'Éducation.

Il est recommandé d'activer, dans la mesure du possible, les trois protocoles pour optimiser la réduction des risques.

Dans la suite du document vont être décrites les problématiques et recommandations autour des protocoles SPF, DKIM et DMARC du point de vue des infrastructures envoyant les messages. Il est à noter qu'il est important, pour une parfaite efficacité des mécanismes, de configurer aussi les systèmes antipourriel récepteurs afin qu'ils prennent en compte les trois protocoles décrits.

Étant donné le nombre de solutions supportant ces protocoles et la diversité de contextes pouvant influer leurs implémentations, il n'est pas possible de détailler les éléments de configuration dans cette instruction.

Stratégie et considérations:

La mise en place des protocoles SPF, DKIM et DMARC est une bonne pratique en Sécurité. Ils constituent une brique importante dans la sécurisation des échanges et permettront de réduire le risque d'usurpation de l'identité de votre organisation. Déployés largement, ils permettront de réduire significativement les risques liés à l'hameçonnage.

Il est important d'assimiler que l'implémentation de SPF, DKIM et DMARC relève d'une stratégie et nécessite aussi des compétences techniques en messagerie. Plusieurs phases de configuration et d'organisation sont à anticiper :

- S'assurer techniquement que les solutions en émissions et réceptions supportent les protocoles;
- Identifier les domaines et sous-domaines utilisés par la messagerie (et globalement aussi);
- Identifier les fournisseurs de domaines;
- Identifier les organismes tiers légitimes pouvant envoyer des courriels au nom de votre organisation;
- Comprendre le fonctionnement de votre infrastructure de messagerie et identifier les serveurs MTA;
- Anticiper la mise en place d'une gestion de clés dans le cadre de DKIM.

En fonction des résultats précédents et des contraintes identifiées, une stratégie de déploiement pourra alors être envisagée. Il peut notamment être décidé d'un redécoupage des sous-domaines par utilisation afin de faciliter leur gestion ou de protéger en priorité uniquement certains d'entre eux.

Il est assez courant de rencontrer des cas non anticipés pouvant amener de faux positifs (tiers inconnus, transferts automatiques, ajout d'entêtes ou de signatures, etc.), il est donc important de procéder par étapes et de passer par des phases de tests en utilisant des politiques peu restrictives au début.

À noter que SPF et/ou DKIM sont des prérequis à DMARC. Il est donc important de procéder d'abord à leur déploiement. De plus, le déploiement de SPF et DMARC peut également être pertinent pour des domaines non dédiés à la messagerie afin d'éviter une utilisation frauduleuse dans ce cadre.

Pour conclure, le déploiement des trois protocoles relève donc plus d'un défi organisationnel que technique.

SPF (Sender Policy Framework):

Comment fonctionne SPF?

SPF détermine les adresses IP autorisées à émettre des courriels selon le domaine associé. Ces adresses IP sont déclarées pour chaque domaine et sous-domaine dans un enregistrement TXT sur le serveur DNS faisant autorité. De cette façon, lorsque le serveur de messagerie du destinataire reçoit un message :

1. Il récupère l'adresse présente dans le « from » de l'enveloppe du courriel;
2. Il vérifie si l'IP source est déclaré comme légitime dans l'enregistrement SPF du DNS;

3. Selon le cas, indique que le message est suspect ou préconise le blocage (dépendant de la stratégie déclarée dans l'enregistrement DNS).

Un exemple d'enregistrement pour « education.gouv.qc.ca »:

```
"v=spf1 mx ip4:205.236.3.145 ip4:167.89.33.215 ip4:204.19.45.226 a:ancmail2.education.gouv.qc.ca
a:sortie1.education.gouv.qc.ca a:sortie2.education.gouv.qc.ca a:sortie3.education.gouv.qc.ca
include:spf.protection.outlook.com include:spf.exclaimer.net -all"
```

Spécifications techniques de SPF : https://tools.ietf.org/html/rfc7208

Quelles sont les limitations?

SPF ne vérifie que le « from » de l'enveloppe et non le « from » de l'entête qui sera affiché par défaut à l'utilisateur par les clients de messagerie. Ceci autorise donc un attaquant à déclarer dans l'enveloppe une adresse source sous son contrôle et usurper une adresse de confiance dans l'entête afin de tromper l'utilisateur tout en passant le contrôle de SPF avec succès.

Comment configurer SPF?

SPF est simple à mettre en place. Il repose sur un enregistrement DNS à définir pour le domaine utilisé pour votre messagerie. Il est souvent activé par défaut cependant, il peut s'avérer nécessaire de mettre à jour les enregistrements dans certains cas : sources d'envois multiples, domaines spécifiques, architecture hybride ou nécessité d'activer d'autres protocoles.

Il est recommandé de passer par les étapes suivantes concernant l'implantation:

1. Faire le bilan des sources de messages et des domaines;
2. Concevoir les enregistrements TXT SPF;
3. Mettre à jour les enregistrements aux fins de tests;
4. Valider les tests et officialiser la pratique.

Lors de la mise en place de SPF, il est fortement encouragé de vérifier la validité de l'enregistrement avant de le mettre en place. Des outils comme mxtoolbox peuvent le permettre : https://mxtoolbox.com/spf.aspx

Il est aussi recommandé de tester les déploiements pour identifier les non-conformités ou placer les messages non vérifiés en quarantaine ou les marquer plutôt que de les abandonner. En effet, de faux positifs peuvent être observés lorsque des sources inconnues, mais légitimes d'envoi sont découvertes (internes, infonuagiques, partenaires, etc.) ou que des transferts automatiques sont configurés.

Voici un article détaillé de Microsoft concernant la mise en place de SPF : https://docs.microsoft.com/fr-fr/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing?view=o365-worldwide

DKIM (DomainKeys Identified Mail):

Comment fonctionne DKIM?

DKIM permet une authentification de la source d'envoi d'un courriel via des moyens cryptographiques. Il repose de nouveau sur la publication d'un enregistrement DNS, mais aussi sur la configuration des serveurs d'envoi.

Un message sera authentifié par une signature cryptographique placée en entête et vérifiée à la réception. Ce protocole permet de nous assurer que le domaine n'a pas été usurpé, mais aussi que le message n'a pas été altéré.

Le protocole fonctionnera de la façon suivante :

1. Le courriel sortant et une partie de ses entêtes sont signés cryptographiquement par le MTA (serveur de transfert de courrier) du domaine au moyen d'une clé privée. Toute modification du courriel à partir de ce point entrainera son invalidation. La signature est ajoutée dans un entête du courriel.
2. À la réception du MTA destinataire, la signature de l'entête DKIM sera extraite et la clé publique du domaine présent dans l'entête « from » récupéré du DNS pour procéder à sa vérification.
3. Si l'authenticité et l'intégrité du message sont vérifiées, le protocole valide le message.

À noter que comme SPF, DKIM n'offre pas de mécanismes de blocage. Il propose une aide afin de déterminer si un message est usurpé.

Un enregistrement DNS pour DKIM ressemble à cela :

```
"dk1024-2012._domaine.exemple.com.  600  IN  TXT  "v=DKIM1\;
p=MIGfaA10CSqPSIb3pQEBAQAAA4GNADCBiQKBgCC1DaNgLlSyQMNWVLNLvyY/neDgaL… "
```

Spécifications techniques de DKIM : https://tools.ietf.org/html/rfc6376

Quelles sont les limitations?

Le protocole DKIM est très intéressant au niveau sécurité, mais ne permet malheureusement pas une protection parfaite. En effet, il a été révélé que le protocole ne protège pas contre les rejeux de messages, car toutes les parties du message ne sont pas signées et des entêtes peuvent être ajoutés sans incidence pour le protocole. DKIM ne valide que le fait que le domaine envoyant le message initialement est bien le bon domaine.

Comment configurer DKIM?

Même s'il est un peu plus complexe à gérer que SPF en raison de modification à apporter côté serveurs d'envoi, de nombreux systèmes supportent DKIM nativement (Microsoft 365, GSuite, etc.). Si le vôtre le permet, il est particulièrement intéressant de l'implémenter en raison des contrôles qu'il permet.

Les mêmes recommandations et prérequis de déploiement que SPF sont applicables ici.

De plus, il est nécessaire de générer une paire de clés cryptographiques pour chacun des domaines couverts par DKIM puis de publier la clé publique dans un enregistrement DNS via votre hébergeur de domaine. Il faudra ensuite activer DKIM au niveau de l'infrastructure de messagerie et fournir la clé privée à chaque MTA.

Il est important de noter qu'une modification après signature invalidera la vérification. Un ajout de signature automatique ou d'un entête posera donc potentiellement problème. Il faut veiller que tout ajout se fasse avant traitement.

Votre enregistrement DNS peut être vérifié ici : https://mxtoolbox.com/dkim.aspx

Voici un article détaillé par Microsoft notamment dans le cadre de Microsoft 365 : https://docs.microsoft.com/fr-fr/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide

DMARC (Domain-based Message Authentification, Reporting and Conformance) :

Comment fonctionne DMARC?

DMARC a été créé de façon à répondre en partie aux limitations posées par SPF et DKIM. Il vient donc en complément de ces protocoles pour apporter une solution plus complète et maîtrisable face à l'usurpation.

DMARC va permettre de vérifier la correspondance entre les domaines des champs « from » de l'entête et de l'enveloppe pour SPF et DKIM et préciser les actions à entreprendre en cas d'échec.

DMARC va fonctionner également via la publication d'un enregistrement DNS. Trois actions possibles sont prévues par le protocole en cas d'échec de vérification :

- Aucune (none) : Mode surveillance;
- Quarantaine (Quarantine) : Courriel livré, mais marqué comme « suspect »;
- Rejeter (reject) : Courrier bloqué.

Pour être livré, le courriel doit valider au moins l'une des vérifications de SPF et DKIM et les champs « from » doivent correspondre.

Le protocole offre aussi un mécanisme permettant au propriétaire de domaine de recevoir des rapports faisant état des courriels identifiant leur domaine. Ce rapport est envoyé à l'adresse indiquée dans l'enregistrement DNS. Ceci permet de suivre la livraison des courriels envoyés depuis votre domaine, contrôler le déploiement de SPF et DKIM et identifier les auteurs malveillants envoyant les courriels en usurpant le nom de votre domaine ou même des sources légitimes, mais inconnues.

Un enregistrement TXT pour DMARC ressemble à ceci :

```
"TXT IN "v=DMARC1;p=reject;pct=100;rua=mailto:dmarc@exemple.com;""
```

Spécificités techniques de DMARC: https://tools.ietf.org/html/rfc7489

Comment configurer DMARC?

DMARC se base sur SPF et/ou DKIM en y apportant des contrôles supplémentaires. Il faudra donc passer par une implémentation de ces protocoles avant de passer à la partie DMARC à proprement parler. À noter que les prérequis et précautions seront semblables pour les trois protocoles.

Il est notamment très important d'identifier vos domaines, sous-domaines et serveurs DNS. Il est conseillé de passer par plusieurs étapes de validations du bon déploiement et fonctionnement de votre stratégie SPF/DKIM/DMARC avant de passer sur un mode bloquant étendu à l'ensemble de votre organisation.

Comme déjà indiqué, ceci impliquera donc une gestion de projet et des compétences techniques en messagerie afin de faire les bons choix en termes de stratégie.

En effet, les mêmes problématiques autour des expéditeurs tiers et des transferts de messages automatiques vont être à anticiper ici aussi, car ils peuvent faire échouer les vérifications. Une réflexion autour des domaines à utiliser, d'utilisation d'enregistrements CNAME, d'un découpage par utilisation voire d'une sélection concernant l'utilisation de DKIM ou SPF suivant les contraintes feront partie des considérations du projet.

Il est important de compter sur le mécanisme de rapport autorisé par DMARC afin de pouvoir identifier les problèmes et réajuster les stratégies.

Voici un article de Microsoft détaillant l'implémentation de DMARC : https://docs.microsoft.com/fr-fr/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide#how-microsoft-365-handles-inbound-email-that-fails-dmarc

Pour aller plus loin :

Description complète (à partir de page 24) :
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf

Directives de mise en œuvre du CCC : https://www.cyber.gc.ca/fr/orientation/directives-de-mise-en-oeuvre-protection-du-domaine-de-courrier

Liens utiles, conseils et détails pour configurer les protocoles dans diverses solutions : https://www.globalcyberalliance.org/dmarc-implementation-guides/

chapitre A-2.1

LOI SUR L'ACCES AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

9. Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public.

Ce droit ne s'étend pas aux notes personnelles inscrites sur un document, ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature.

1982, c. 30, a. 9.

14. Un organisme public ne peut refuser l'accès à un document pour le seul motif que ce document comporte certains renseignements qu'il doit ou peut refuser de communiquer en vertu de la présente loi.

Si une demande porte sur un document comportant de tels renseignements, l'organisme public peut en refuser l'accès si ces renseignements en forment la substance. Dans les autres cas, l'organisme public doit donner accès au document demandé après en avoir extrait uniquement les renseignements auxquels l'accès n'est pas autorisé.

1982, c. 30, a. 14.

22. Un organisme public peut refuser de communiquer un secret industriel qui lui appartient.

Il peut également refuser de communiquer un autre renseignement industriel ou un renseignement financier, commercial, scientifique ou technique lui appartenant et dont la divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à l'organisme ou de procurer un avantage appréciable à une autre personne.

Un organisme public constitué à des fins industrielles, commerciales ou de gestion financière peut aussi refuser de communiquer un tel renseignement lorsque sa divulgation risquerait vraisemblablement de nuire de façon substantielle à sa compétitivité ou de révéler un projet d'emprunt, de placement, de gestion de dette ou de gestion de fonds ou une stratégie d'emprunt, de placement, de gestion de dette ou de gestion de fonds.

1982, c. 30, a. 22; 2006, c. 22, a. 11.

28. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement contenu dans un document qu'il détient dans l'exercice d'une fonction, prévue par la loi, de prévention, de détection ou de répression du crime ou des infractions aux lois ou dans l'exercice d'une collaboration, à cette fin, avec une personne ou un organisme chargé d'une telle fonction, lorsque sa divulgation serait susceptible:

1° d'entraver le déroulement d'une procédure devant une personne ou un organisme exerçant des fonctions juridictionnelles;

2° d'entraver une enquête à venir, en cours ou sujette à réouverture;

3° de révéler une méthode d'enquête, une source confidentielle d'information, un programme ou un plan d'action destiné à prévenir, détecter ou réprimer le crime ou les infractions aux lois;

4° de mettre en péril la sécurité d'une personne;

5° de causer un préjudice à une personne qui est l'auteur du renseignement ou qui en est l'objet;

6° de révéler les composantes d'un système de communication destiné à l'usage d'une personne chargée d'assurer l'observation de la loi;

7° de révéler un renseignement transmis à titre confidentiel par un corps de police ayant compétence hors du Québec;

8° de favoriser l'évasion d'un détenu; ou

9° de porter atteinte au droit d'une personne à une audition impartiale de sa cause.

Il en est de même pour un organisme public, que le gouvernement peut désigner par règlement conformément aux normes qui y sont prévues, à l'égard d'un renseignement que cet organisme a obtenu par son service de sécurité interne, dans le cadre d'une enquête faite par ce service et ayant pour objet de prévenir, détecter ou réprimer le crime ou les infractions aux lois, susceptibles d'être commis ou commis au sein de l'organisme par ses membres, ceux de son conseil d'administration ou de son personnel ou par ceux de ses agents ou mandataires, lorsque sa divulgation serait susceptible d'avoir l'un des effets mentionnés aux paragraphes 1° à 9° du premier alinéa.

1982, c. 30, a. 28; 1990, c. 57, a. 7; 2006, c. 22, a. 14.

29. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi.

Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

1982, c. 30, a. 29; 2006, c. 22, a. 16.

34. Un document du bureau d'un membre de l'Assemblée nationale ou un document produit pour le compte de ce membre par les services de l'Assemblée n'est pas accessible à moins que le membre ne le juge opportun.

Il en est de même d'un document du cabinet du président de l'Assemblée, d'un membre de celle-ci visé dans le premier alinéa de l'article 124.1 de la Loi sur l'Assemblée nationale (chapitre A-23.1) ou d'un ministre visé dans l'article 11.5 de la Loi sur l'exécutif (chapitre E-18), ainsi que d'un document du cabinet ou du bureau d'un membre d'un organisme municipal ou scolaire.

1982, c. 30, a. 34; 1982, c. 62, a. 143; 1983, c. 55, a. 132; 1984, c. 47, a. 1.

37. Un organisme public peut refuser de communiquer un avis ou une recommandation faits depuis moins de dix ans, par un de ses membres, un membre de son personnel, un membre d'un autre organisme public ou un membre du personnel de cet autre organisme, dans l'exercice de leurs fonctions.

Il peut également refuser de communiquer un avis ou une recommandation qui lui ont été faits, à sa demande, depuis moins de dix ans, par un consultant ou par un conseiller sur une matière de sa compétence.

1982, c. 30, a. 37.

39. Un organisme public peut refuser de communiquer une analyse produite à l'occasion d'une recommandation faite dans le cadre d'un processus décisionnel en cours, jusqu'à ce que la recommandation ait fait l'objet d'une décision ou, en l'absence de décision, qu'une période de cinq ans se soit écoulée depuis la date où l'analyse a été faite.

1982, c. 30, a. 39.

41. Le vérificateur général ou une personne exerçant une fonction de vérification dans un organisme public ou pour le compte de cet organisme peut refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation serait susceptible:

1° d'entraver le déroulement d'une opération de vérification;

2° de révéler un programme ou un plan d'activité de vérification;

3° de révéler une source confidentielle d'information relative à une vérification; ou

4° de porter sérieusement atteinte au pouvoir d'appréciation accordé au vérificateur général par les articles 38, 39, 40, 42, 43, 43.1 et 45 de la Loi sur le vérificateur général (chapitre V-5.01).

1982, c. 30, a. 41; 1985, c. 38, a. 82; 2006, c. 3, a. 18.

§ 7. — *Restrictions inapplicables*

2006, c. 22, a. 22.

48. Lorsqu'il est saisi d'une demande qui, à son avis, relève davantage de la compétence d'un autre organisme public ou qui est relative à un document produit par un autre organisme public ou pour son compte, le responsable doit, dans le délai prévu par le premier alinéa de l'article 47, indiquer au requérant le nom de l'organisme compétent et celui du responsable de l'accès aux documents de cet organisme, et lui donner les renseignements prévus par l'article 45 ou par le deuxième alinéa de l'article 46, selon le cas.

Lorsque la demande est écrite, ces indications doivent être communiquées par écrit.

1982, c. 30, a. 48.

53. Les renseignements personnels sont confidentiels sauf dans les cas suivants:
1° la personne concernée par ces renseignements consent à leur divulgation; si cette personne est mineure, le consentement peut également être donné par le titulaire de l'autorité parentale;
2° ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.

1982, c. 30, a. 53; 1985, c. 30, a. 3; 1989, c. 54, a. 150; 1990, c. 57, a. 11; 2006, c. 22, a. 29.

54. Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.

1982, c. 30, a. 54; 2006, c. 22, a. 110.

56. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne.

1982, c. 30, a. 56; 2006, c. 22, a. 110.

59. Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée.

Toutefois, il peut communiquer un tel renseignement sans le consentement de cette personne, dans les cas et aux strictes conditions qui suivent:
1° au procureur de cet organisme si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi que cet organisme est chargé d'appliquer, ou au Directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
2° au procureur de cet organisme, ou au procureur général lorsqu'il agit comme procureur de cet organisme, si le renseignement est nécessaire aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe 1°;
3° à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
4° à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;
5° à une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique;
6° *(paragraphe abrogé);*
7° *(paragraphe abrogé);*
8° à une personne ou à un organisme, conformément aux articles 61, 66, 67, 67.1, 67.2, 68 et 68.1;
9° à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement.

1982, c. 30, a. 59; 1983, c. 38, a. 55; 1984, c. 27, a. 1; 1985, c. 30, a. 5; 1987, c. 68, a. 5; 1990, c. 57, a. 13; 2006, c. 22, a. 32; 2005, c. 34, a. 37.

127. La Commission peut, de sa propre initiative ou sur la plainte d'une personne intéressée, faire enquête sur:
1° un fichier confidentiel pour déterminer si les renseignements personnels qui s'y trouvent ont été versés et utilisés conformément au décret;
2° le respect de la confidentialité des renseignements personnels contenus dans un dossier ayant trait à l'adoption d'une personne et détenu par un organisme public;
3° le respect de la confidentialité des renseignements personnels contenus dans le dossier que détient le curateur public sur une personne qu'il représente ou dont il administre les biens.

L'enquête est secrète. Seul un membre de la Commission ou un membre de son personnel de direction désigné par écrit à cette fin par la Commission peut prendre connaissance des renseignements personnels versés au fichier ou des renseignements personnels contenus dans un dossier visé aux paragraphes 2° et 3° du premier alinéa. Toutefois, un membre du personnel de la Commission peut, si la Commission l'autorise par écrit, prendre connaissance des renseignements personnels contenus dans un dossier visé aux paragraphes 2° et 3° du premier alinéa.

1982, c. 30, a. 127; 1987, c. 68, a. 11; 1989, c. 54, a. 152; 2006, c. 22, a. 110.

Avis de recours

À la suite d'une décision rendue en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (la Loi).

Révision par la Commission d'accès à l'information

a) *Pouvoir* :

L'article 135 de la Loi prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision. La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

Québec	525, boul René-Lévesque Est Bureau 2.36 Québec (Québec) G1R 5S9	Tél. : 418 528-7741 Numéro sans frais 1 888 528-7741	Téléc. : 418 529-3102
Montréal	500, boul. René-Lévesque Ouest Bureau 18.200 Montréal (Québec) H2Z 1W7	Tél. : 514 873-4196 Numéro sans frais 1 888 528-7741	Téléc. : 514 844-6170

b) *Motifs* :

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) *Délais* :

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).