Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Pratiques exemplaires en matière de sécurité pour le courrier électronique

Série Gestionnaires

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer avec nous par téléphone au 613-949-7048 ou au 1-833-CYBER-88 ou par courriel à l'adresse contact@cyber.gc.ca.

Date d'entrée en vigueur

Le présent document entre en vigueur le 21 août 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version.	*21* août *2025*

D97-4/60-002-2025F-PDF
ISBN 978-0-660-78521-9

Vue d'ensemble

Dans le contexte numérique actuel, il est essentiel pour votre organisation de protéger les données sensibles. Bien que le courrier électronique soit un moyen de communication fondamental, il est susceptible à diverses menaces. Le courrier électronique sert de canal principal pour l'échange d'information, ce qui signifie que votre organisation se doit de mettre en œuvre des mesures de sécurité robustes pour la protection des données. La présente publication offre des conseils à propos des pratiques et des protocoles de sécurité d'importance liés au courrier électronique que votre organisation devrait adopter dans le but de renforcer ses capacités de défense et de préserver la confidentialité, l'intégrité et la disponibilité de ses communications et de ses données. Cette publication aidera votre organisation à mettre en œuvre des mesures de protection telles que le chiffrement, l'authentification et des passerelles sécurisées. En plus des mesures de protection, il est également important d'améliorer la sensibilisation et la conformité des membres du personnel aux exigences et aux pratiques exemplaires en matière de cybersécurité. Collectivement, ces mesures permettront à votre organisation de naviguer avec confiance dans l'espace numérique, tout en assurant la sécurité et la confidentialité de son information sensible.

Table des matières

1 Introduction

Le courrier électronique est un outil de communication important pour les personnes et les organisations, et il est utilisé à grande échelle sur divers appareils. Dans les activités organisationnelles de technologies de l'information (TI), le courrier électronique est particulièrement important pour les communications opérationnelles internes et externes. Son utilisation étendue en fait une cible de choix pour les auteurs de menace, qui souhaitent exploiter les vulnérabilités et compromettre les données sensibles. Cependant, le courrier électronique n'a pas été conçu initialement en tenant compte de la sécurité et de la confidentialité. Les technologies que nous utilisons de nos jours qui améliorent la sécurité des courriels, comme le chiffrement et les protocoles d'authentification, ont été ajoutées ultérieurement afin d'atténuer les risques associés aux communications par courriel.

Les auteurs de menace perfectionnent continuellement leurs tactiques pour exploiter les vulnérabilités liées au courrier électronique. Ainsi, l'établissement d'une défense solide en appliquant une gamme complète de mesures de sécurité au courrier électronique permettra de préserver la confidentialité, la vie privée et l'intégrité de vos communications numériques. Les comptes de courrier électronique hébergent une grande quantité de renseignements privés, y compris des données personnelles, des détails financiers et des échanges commerciaux confidentiels. Il est donc important de bien sécuriser les communications par courriel pour prévenir les intrusions qui risquent de compromettre l'intégrité des échanges. La sécurité du courrier électronique offre également une protection contre les attaques par maliciel et par hameçonnage, qui sont souvent amorcées au moyen de courriels trompeurs. De plus, veiller à la disponibilité des systèmes de courrier électronique est un aspect crucial de la sécurité des courriels, afin d'éviter les interruptions, les périodes d'indisponibilité et les pertes de données potentielles qui pourraient survenir à la suite d'attaques contre des systèmes vulnérables.

Pour de nombreuses organisations et entreprises, le respect de la réglementation de l'industrie et des normes de conformité est essentiel pour éviter les répercussions juridiques et pour protéger la réputation. En établissant des mesures de sécurité robustes pour le courrier électronique, vous pourrez mieux démontrer votre conformité et votre traitement adéquat de la confidentialité, de l'intégrité et de la disponibilité de l'information sensible de votre clientèle et de vos partenaires.

1.1 Menaces courantes liées au courrier électronique

Bien que le courrier électronique soit un outil de communication largement répandu, il présente des risques. Les menaces liées au courrier électronique sont diversifiées, allant de stratagèmes d'hameçonnage à des maliciels, et évoluent sans cesse. La section suivante traitera de certaines menaces courantes qui peuvent compromettre l'information privée et la sécurité numérique de votre organisation.

1.1.1 Hameçonnage

Une attaque par hameçonnage est une tactique trompeuse utilisée par les auteurs de menace qui vise à envoyer des courriels d'apparence légitime à des utilisatrices et utilisateurs. Elle représente la menace la plus courante pour la sécurité des courriels. Relativement facile à détecter par le passé, les attaques par hameçonnage se sont raffinées au fil du temps. Avec l'arrivée de l'intelligence artificielle (IA), les courriels d'hameçonnage contiennent de moins en moins d'erreurs d'orthographe, de tropes ou de leurres typiques. Ils sont désormais bien rédigés et leur contenu semble légitime, ce qui les rend encore plus difficiles à détecter.

Les attaques par hameçonnage peuvent être génériques ou ciblées. Dans le cas des attaques ciblées, aussi connues sous le nom de harponnage, les auteurs de menace effectuent des recherches approfondies sur des personnes ou des groupes particuliers qui détiennent un accès privilégié à de l'information de valeur, pour ensuite concevoir des courriels pertinents qui n'éveilleront pas de soupçon.

La chasse à la baleine est une forme particulière de harponnage dans le cadre de laquelle les auteurs de menace visent des personnes haut placées au sein d'une organisation et se font passer pour des autorités de confiance. L'objectif principal reste toutefois le même : manipuler les utilisatrices et utilisateurs afin qu'ils dévoilent de l'information sensible, comme des noms d'utilisateur, des mots de passe et des renseignements bancaires. Les auteurs de menace peuvent également inciter les utilisatrices et utilisateurs à cliquer sur des liens malveillants, à ouvrir des pièces jointes dangereuses ou à apporter des modifications non autorisées à un système auquel ils ont accès. Il est donc essentiel de rester vigilant et de comprendre l'évolution des attaques par hameçonnage afin de protéger votre organisation de ces menaces.

Pour de plus amples renseignements sur les attaques par hameçonnage, les courriels malveillants et les moyens de les éviter, de les repérer et de les traiter, lisez les publications suivantes :

- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Reconnaître les courriels malveillants (ITSAP.00.100)

1.1.2 Usurpation d'adresse électronique

L'usurpation d'adresse électronique est une tactique trompeuse où les auteurs de menace manipulent les détails de l'expéditeur dans l'en-tête d'un courriel de manière à ce que celui-ci semble provenir d'une source fiable. Cette pratique vise principalement à déjouer les destinataires afin qu'ils croient que le courriel est légitime et ainsi les inciter à l'ouvrir et à interagir avec le contenu.

Le danger inhérent de l'usurpation d'adresse électronique est que les messages trompeurs contiennent généralement des maliciels, des virus ou des liens malveillants qui redirigent les utilisatrices et utilisateurs vers de faux sites ou services. Le simple fait d'ouvrir le courriel peut exposer l'appareil du destinataire à des menaces et le rendre vulnérable à de plus amples exploitations. L'usurpation d'adresse électronique est couramment employée dans le cadre d'attaques par hameçonnage et d'escroqueries par faux ordre de virement. Les ramifications de ces attaques dépassent largement les dommages immédiats. La divulgation d'information sensible découlant d'un courriel mystifié peut mener à un vol d'identité.

Afin d'atténuer les risques associés à l'usurpation d'adresse électronique, prenez l'habitude de toujours passer votre souris sur les liens dans un courriel avant de cliquer sur ceux-ci. Vous pourrez ainsi vérifier l'adresse URL réelle et vous assurer qu'elle correspond au domaine attendu et qu'elle est légitime. Évitez de cliquer sur des liens qui semblent suspects ou inconnus. Consultez toujours l'équipe responsable de la sécurité des TI de votre organisation si vous avez des doutes. Vous devez aussi examiner tout courriel qui contient des demandes atypiques, comme une transaction financière urgente ou une demande d'information sensible. Il est prudent de vérifier ces demandes en utilisant d'autres canaux de communication, comme un appel téléphonique à l'expéditeur ou une consultation manuelle du site Web en question dans votre navigateur afin de confirmer les déclarations faites dans le courriel.

Un autre point important à considérer concerne les attaques par homographe, où les auteurs de menace utilisent des caractères appartenant à d'autres alphabets, comme le cyrillique ou le grec, mais qui ressemblent à des caractères romains, afin de créer des adresses courriel ou URL trompeuses. Accordez une attention particulière aux différences subtiles de caractère qui peuvent indiquer une tentative d'usurpation d'adresse électronique. En combinant ces stratégies, vous pourrez mieux vous protéger des risques associés à l'usurpation d'adresse électronique.

1.1.3 Maliciels

Les auteurs de menace utilisent souvent le courrier électronique pour transmettre différents types de maliciels, comme des virus, des vers, des rançongiciels ou des logiciels espions. Les maliciels peuvent être directement joints à des courriels ou intégrés à des documents partagés, puis envoyés à titre de fichier joint ou de lien, ou au moyen d'un stockage infonuagique. Une fois que le maliciel s'est infiltré dans l'appareil de l'utilisatrice ou utilisateur, il peut obtenir un accès non autorisé aux composants du système, compromettre ou voler de l'information sensible et chiffrer des fichiers. Pour de plus amples renseignements sur les façons de se défendre contre une attaque par rançongiciel et de se rétablir après coup, lisez la publication Guide sur les rançongiciels (ITSM.00.099).

1.1.4 Escroquerie par faux ordre de virement

Les escroqueries par faux ordre de virement sont une préoccupation grandissante pour les organisations, peu importe la taille et le secteur. Ce modèle sophistiqué d'attaque cible souvent les entreprises offrant des services de virements bancaires. Les auteurs de menace tentent d'escroquer les organisations en se faisant passer pour des cadres supérieures et supérieurs ou des partenaires commerciaux dans le but de tromper les membres du personnel, le but ultime étant que leurs cibles virent des fonds à des comptes frauduleux.

Ces attaques ciblées et planifiées avec soin impliquent d'importantes sommes d'argent et représentent ainsi l'une des menaces les plus dommageables financièrement pour la sécurité du courrier électronique. Bien que les auteurs d'escroqueries par faux ordre de virement puissent exploiter et voler des données, ils visent principalement à s'enrichir et, pour ce faire, tentent de tromper le personnel des organisations en faisant appel à des tactiques de piratage psychologique, comme l'usurpation d'identité. Pour de plus amples renseignements sur les façons de protéger votre organisation contre le piratage psychologique, lisez le document Piratage psychologique (ITSAP.00.166).

1.1.5 Usurpation d'identité

Les auteurs de menace utilisent l'usurpation d'identité afin d'exploiter la confiance, de faire des profits ou d'accéder à de l'information sensible grâce au courrier électronique. Par exemple, dans le cas des escroqueries par faux ordre de virement, les auteurs de menace se font passer pour des personnes de confiance, comme des membres du personnel, afin de voler de l'argent aux entreprises ou à leurs clients et partenaires. Une attaque par usurpation de l'identité d'une avocate ou d'un avocat est un autre exemple. Dans ce contexte, l'attaquante ou attaquant prétend être une représentante ou un représentant juridique et cible souvent des membres du personnel ne disposant pas des connaissances ou de l'autorité nécessaires pour vérifier la légitimité de la demande. De façon similaire, les auteurs de menace se font parfois passer pour des entités faisant autorité, comme des organismes de réglementation, des ministères gouvernementaux et des organismes d'application de la loi.

L'usurpation d'une marque est une autre tactique employée par les auteurs de menace. Ils s'associent faussement à une marque bien connue pour déjouer la ou le destinataire afin qu'il révèle de l'information confidentielle. Il existe de nombreuses techniques d'usurpation d'identité, comme se faire passer pour du personnel interne pour commettre une fraude financière ou exploiter la crédibilité de marques réputées à des fins illicites. Il est donc très important d'adopter des pratiques de sécurité axées sur la vigilance pour le courrier électronique.

1.1.6 Exfiltration de données

L'exfiltration de données consiste à transférer ou à retirer de l'information sensible d'un système de courrier électronique organisationnel sans autorisation. Les auteurs de menace utilisent différentes techniques, comme l'hameçonnage, les logiciels espions ou les maliciels afin d'exfiltrer des données. Ces attaques exposent les organisations à des cybercrimes potentiels, y compris l'extorsion et la vente illicite de données sur le Web clandestin. Par conséquent, ces attaques peuvent avoir des conséquences importantes sur les activités d'une organisation, y compris des atteintes coûteuses à la protection des données ou des répercussions juridiques. Pour en apprendre davantage sur les façons de protéger vos données contre l'exfiltration de données, lisez la publication Défense contre les menaces d'exfiltration de données (ITSM.40.110).

1.1.7 Pourriels

Les entreprises emploient fréquemment les pourriels (des messages non sollicités) comme moyen pour promouvoir leurs biens, leurs services ou leurs sites Web à des fins commerciales. Bien que les pourriels ne soient pas considérés comme étant aussi préoccupants que d'autres menaces pour la sécurité du courrier électronique, ils présentent néanmoins des risques de sécurité inhérents. Généralement, les fournisseurs de services de courrier électronique détectent et filtrent les pourriels, mais ces messages représentent tout de même une menace, car certains courriels contenant des liens ou des fichiers joints malveillants peuvent échapper au filtre des fournisseurs.

2 Protocoles de sécurité du courrier électronique

Les protocoles de sécurité du courrier électronique sont importants pour protéger les communications numériques, car ils empêchent l'accès non autorisé au contenu des courriels. Ces protocoles établissent les règles et les normes qui régissent la transmission, la réception et le traitement des courriels entre les serveurs et les clients. En établissant des étapes et des règles précises pour l'expédition, la réception, le stockage et la récupération des courriels, les protocoles permettent d'établir un processus sécurisé de communication par courriel.

Cette section présente un aperçu de quelques protocoles bien établis permettant d'améliorer la sécurité des courriels. L'intégration de ces protocoles et des pratiques de sécurité des courriels vous permettra de créer une ligne de défense complète, dotée de plusieurs couches, contre de nombreuses menaces, et d'assurer la confidentialité, l'intégrité et la disponibilité de vos communications par courriel. La publication du Centre pour la cybersécurité Directives de mise en œuvre – protection du domaine de courrier (ITSP.40.065 v1.1) présente des conseils sur la mise en œuvre de mesures de sécurité techniques pour protéger les domaines de votre organisation de l'usurpation d'adresse électronique.

2.1 Protocole TLS

Le protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*), qui remplace le protocole SSL (*Secure Sockets Layer*), est un protocole cryptographique permettant d'établir un canal de communication sécurisé au moyen de l'établissement d'une liaison. Lors de l'établissement d'une liaison TLS, les deux éléments participant à la communication, typiquement le client et le serveur, échangent des clés cryptographiques et chiffre les transmissions de données subséquentes. Bien que les protocoles SSL et les versions plus anciennes du protocole TLS soient considérés comme non sécurisés, la version la plus récente du protocole TLS permet d'assurer la confidentialité des courriels en transit. Ainsi, les courriels qui circulent sur Internet utilisant ce protocole sont chiffrés et protégés des écoutes clandestines. Toutefois, même si le courriel est chiffré durant la transmission, les serveurs de réception et d'expédition peuvent tout de même accéder au message en clair. Par conséquent, le protocole TLS n'assure pas la confidentialité de bout en bout des courriels.

Par ailleurs, un courriel transmis par Internet subit normalement de nombreux transferts intermédiaires en passant par de nombreux serveurs avant d'atteindre sa destination. Bien que le protocole TLS puisse sécuriser le transfert initial, à partir du client de courriel vers le premier serveur, il ne garantit pas que les transferts subséquents utiliseront un chiffrement TLS. Vous ne devez donc pas vous fier uniquement au protocole TLS pour protéger l'information sensible, à moins que vous ayez entièrement confiance en l'infrastructure de réception et en l'organisation exploitant les serveurs de courrier électronique. Cela est particulièrement important lorsque l'on considère la différence entre assurer la sécurité de la communication entre une application client de courrier électronique et un serveur, et assurer la confidentialité de bout en bout entre l'expéditrice ou expéditeur et la ou le destinataire du courriel.

Pour obtenir de l'information sur la configuration du protocole TLS, lisez la publication Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062).

2.2 Protocole S/MIME

Le protocole S/MIME (*Secure/Multipurpose Internet Mail Extensions*) sert à assurer la sécurité des communications par courriel au moyen d'un cadre de chiffrement de bout en bout. Ce protocole utilise une infrastructure à clé publique (ICP) et

un chiffrement asymétrique impliquant une paire de clés mathématiquement liées, soit une clé publique et une clé privée. Ces clés fonctionnent de manière collaborative pour établir un canal sécurisé pour la communication.

Le protocole S/MIME sert à deux fins : signer numériquement les messages et les chiffrer lorsqu'ils sont envoyés par Internet. Les signatures numériques permettent d'authentifier l'identité de l'expéditrice ou expéditeur, alors que le chiffrement permet d'assurer la confidentialité du contenu du courriel. Lors du processus de chiffrement, la clé publique de la ou du destinataire est employée et le déchiffrement requiert l'utilisation de la clé privée correspondante, détenue en exclusivité par le ou le destinataire du message. Ainsi, la ou le destinataire désigné est la seule personne à pouvoir accéder aux données sensibles, pourvu que la clé privée demeure sécurisée. Durant l'authentification, une signature est générée au moyen de la clé privée de l'expéditrice ou expéditeur, et elle peut être vérifiée au moyen de la clé publique correspondante. De cette façon, la ou le destinataire peut vérifier l'authenticité de la source du message.

L'un des principaux avantages du protocole S/MIME est sa résilience contre les activités malveillantes, comme l'usurpation de l'identité de l'expéditeur et l'interception du message. Le protocole S/MIME établit un cadre sécurisé pour expédier et recevoir des messages en exigeant que les clients de courrier électronique détiennent un certificat numérique pour authentifier l'identité de l'expéditrice ou expéditeur et déchiffrer les courriels lors de la transmission.

Même si le protocole S/MIME permet d'améliorer la sécurité des courriels, il est important de savoir que les en-têtes de courriel ne sont pas chiffrés. Les auteurs de menace pourraient donc avoir accès à de l'information sur l'expéditrice ou expéditeur et la ou le destinataire. La publication du Centre pour la cybersécurité Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) offre des conseils sur la configuration des protocoles TLS et S/MIME.

2.3 Protocoles PGP et OpenPGP

Le protocole PGP (*Pretty Good Privacy*), y compris le protocole de source ouverte OpenPGP (*Open-Source Pretty Good Privacy*), assure le chiffrement de bout en bout du texte en clair, des courriels et des fichiers, ce qui limite l'accès à la ou au destinataire prévu. Le protocole emploie des signatures numériques pour vérifier l'authenticité de l'expéditrice ou expéditeur et un mécanisme de chiffrement à clé publique ainsi qu'un système de gestion de clés dans le but de sécuriser les communications. Le coût de la mise en œuvre de PGP est relativement faible, et il existe de nombreuses solutions logicielles PGP gratuites et de source ouverte.

Il est toutefois important de noter que le protocole PGP exige que l'expéditrice ou expéditeur ainsi que la ou le destinataire disposent d'un logiciel compatible en mesure de chiffrer et de déchiffrer les messages pour que les mécanismes cryptographiques fonctionnent adéquatement. De plus, les deux parties doivent échanger leur clé publique avec l'autre et la stocker. Les anciens courriels, qui n'ont pas été chiffrés à l'origine au moyen d'un logiciel PGP, resteront non chiffrés, sauf s'ils sont envoyés de nouveau en utilisant le processus de chiffrement sécurisé.

Les services de courrier électronique populaires, comme Gmail, Outlook et Yahoo, ne prennent pas en charge nativement le protocole PGP sans l'installation de logiciels supplémentaires ou de compléments additionnels sur le navigateur. Cette restriction peut complexifier la transparence de l'intégration de PGP pour une utilisation quotidienne de la part des utilisatrices et utilisateurs.

En règle générale, le protocole PGP reste un choix rentable et polyvalent pour les personnes et les petites entreprises qui souhaitent profiter de capacités de chiffrement des courriels, pourvu que les exigences de mise en œuvre et de compatibilité soient traitées de manière efficace.

2.3.1 Comparaison des protocoles S/MIME et PGP

Les protocoles S/MIME (*Secure/Multipurpose Internet Mail Extensions*) et PGP (*Pretty Good Privacy*) sont des mécanismes pratiquement identiques en ce qui a trait au traitement du message pour la transmission. La différence importante est que le protocole S/MIME utilise une infrastructure à clé publique (ICP), en prenant soin de souligner le terme « infrastructure ». Le protocole S/MIME exige que toutes les utilisatrices et tous les utilisateurs (expéditrices, expéditeurs et destinataires) possèdent des certificats émis par une autorité de confiance ou déléguée, ce qui permet aux identités des utilisatrices et utilisateurs d'être retracées jusqu'à l'autorité émettrice du certificat. Les certificats S/MIME sont normalement distribués et mis à jour au moyen d'une consultation automatisée à partir d'un annuaire d'entreprise et exigent une infrastructure de soutien.

Par opposition, le protocole PGP utilise des paires de clés publique-privée autogénérées devant être gérées et mises à jour manuellement, ainsi que des relations d'approbation devant faire l'objet d'une vérification personnelle. Par exemple, une partie peut demander la clé publique PGP de l'autre partie avant de lui fournir sa propre clé. Toutefois, cet échange peut être vulnérable aux attaques par interception (AitM pour *Adversary-in-the-Middle*) et d'usurpation d'identité, car l'échange survient avant l'établissement de la relation d'approbation, et donc avant que les deux parties aient échangé les clés pour communiquer entre elles.

Les données au repos sont un autre aspect important de la sécurité des courriels, à la fois pour les protocoles S/MIME et PGP. Les courriels protégés par le protocole TLS sont chiffrés seulement durant la transmission. Une fois que le message atteint sa destination, il est déchiffré et stocké en texte en clair sur le système de la ou du destinataire. Par conséquent, si une personne a accès à votre téléphone cellulaire, à votre ordinateur portable ou au serveur, elle pourra lire tous les messages qui y sont stockés. Toutefois, si les messages sont chiffrés en utilisant le protocole S/MIME ou PGP, ils resteront chiffrés même pendant le stockage, à moins que l'utilisatrice ou utilisateur décide de déchiffrer et de stocker les données en texte en clair.

Il est recommandé que les entreprises et organisations utilisent le protocole S/MIME, car il permet de gérer de manière centralisée les comptes. Par exemple, après le départ d'un membre du personnel, il sera possible de révoquer les justificatifs d'identité ICP de la personne. Par opposition, en utilisant le protocole PGP, il sera nécessaire d'informer tous les autres membres du personnel du départ de la personne et de préciser qu'ils ne peuvent plus faire confiance à leurs justificatifs d'identité PGP, car seule la personne peut révoquer ces clés. En outre, le protocole S/MIME facilite les enquêtes de sécurité, le cas échéant. Les organisations peuvent tenir un registre des communications échangées au moyen du protocole S/MIME, y compris l'horodatage et les données de l'expéditrice ou expéditeur et de la ou du récepteur qui peuvent s'avérer précieux dans le cas des investigations informatiques et de sécurité. Par ailleurs, le protocole S/MIME permet aux administratrices et administrateurs d'appliquer des stratégies liées à la conservation et à l'archivage des messages, assurant ainsi la conformité aux exigences réglementaires et facilitant les activités d'audit et d'investigation en cas d'atteinte à la sécurité ou de problème de conduite. En tirant parti des mécanismes S/MIME pour le chiffrement des courriels et les signatures numériques, les organisations et les entreprises pourront mieux surveiller les activités suspectes et mener des enquêtes connexes, et ainsi renforcer leur posture globale de sécurité et leurs efforts de conformité réglementaire.

2.4 Protocole SPF

Le protocole SPF (*Sender Policy Framework*) est un système qui utilise des fonctions du système d'adressage par domaines (DNS) et qui permet aux propriétaires de domaines de spécifier les serveurs qui sont autorisés à envoyer des courriels au

nom du domaine. Si vous recevez un courriel provenant d'une adresse IP qui n'est pas explicitement autorisée et répertoriée dans l'enregistrement SPF, il n'est probablement pas légitime. Ainsi, lorsqu'un courriel est envoyé, le serveur de courrier électronique de la ou du destinataire consulte l'enregistrement SPF du domaine de l'expéditrice ou expéditeur afin de vérifier si le serveur de courrier électronique de l'expéditrice ou expéditeur figure sur la liste d'autorisation.

Si le serveur de courrier électronique de l'expédition figure dans l'enregistrement SPF (réussite de l'envoi), le courriel est considéré comme légitime et est normalement livré comme il se doit. Toutefois, si le serveur de courrier électronique de l'expédition ne se trouve pas dans l'enregistrement SPF (échec de l'envoi), le serveur de courrier électronique de la ou du destinataire pourra traiter le courriel avec prudence et choisira potentiellement de le rejeter ou de le classer dans le courrier indésirable.

Pour une gestion efficace des stratégies SPF au sein d'une organisation, il est recommandé de commencer par une stratégie d'erreur temporaire (~all) lors des tests initiaux. Cela permet aux administratrices et administrateurs de surveiller et de corriger tous les problèmes de configuration potentiels avant d'appliquer une stratégie de défaillance permanente (-all), qui rejettera catégoriquement les courriels de serveurs non autorisés. De plus, il est important de régler, pour tous les courriels, des domaines et sous-domaines non activés pour le courriel (non-mail-enabled) à une défaillance permanente (-all) pour assurer une protection complète contre les tentatives d'usurpation d'identité pour tous les aspects de la présence numérique de l'organisation.

2.5 Protocole DKIM

Le protocole DKIM (*DomainKeys Identified Mail*) est un mécanisme d'authentification du courrier électronique qui augmente la sécurité des courriels en permettant à l'expéditrice ou expéditeur de signer les courriels. Dans le cadre du processus DKIM, le serveur de courrier électronique génère une signature numérique en utilisant une clé privée, exclusive au propriétaire du domaine, et l'intègre dans l'en-tête de message. Le serveur de la ou du destinataire vérifie ensuite la signature en utilisant la clé publique de l'expéditrice ou expéditeur, extraite à partir des enregistrements DNS, ce qui confirme à la fois l'intégrité de l'expéditrice ou expéditeur et du contenu du message. En particulier, un calcul de valeur de hachage est réalisé à des fins de comparaison pour s'assurer de l'authenticité du message et de l'expéditrice ou expéditeur. Après que le processus de vérification confirme l'identité de l'expéditrice ou expéditeur et l'intégrité du message, le courriel est acheminé à la boîte de réception de la ou du destinataire.

Le protocole DKIM permet ainsi d'assurer l'intégrité des communications par courriel, sans altération des messages. Les serveurs des destinataires doivent vérifier l'authenticité du message et confirmer que celui-ci provient du domaine indiqué, ce qui aide à permet de prévenir les tentatives d'usurpation d'identité et d'adresse électronique.

2.6 Protocole DMARC

Le protocole DMARC (*Domain-Based Message Authentication, Reporting, and Conformance*) aide à prévenir les cas d'hameçonnage et d'usurpation de domaine en permettant aux propriétaires de domaine de définir des protocoles pour le traitement des messages non autorisés ou suspects. Il exploite les protocoles DKIM et SPF pour s'assurer que les courriels sont authentifiés avant la transmission, ce que les courriels proviennent du domaine prévu et qu'ils sont expédiés aux destinataires légitimes.

Une caractéristique importante de DMARC est qu'il permet aux propriétaires de domaine d'établir des stratégies pour les serveurs de réception. Cette fonction facilite un traitement efficace des messages, même s'ils proviennent de sources qui ne sont pas dignes de confiance. Le protocole DMARC guide le serveur en lui indiquant les actions à entreprendre lorsque les messages échouent les vérifications SPF ou DKIM, par exemple les rejeter, les mettre en quarantaine ou les accepter. Certains fournisseurs de courrier électronique d'envergure, comme Gmail et Microsoft, ont mis en œuvre des stratégies DMARC strictes pour les courriels entrants. Ils exigent la réussite des deux vérifications d'authentification (SPF et DKIM) pour les courriels envoyés à partir des domaines qui ont des stratégies DMARC publiées avec des actions de rejet ou de mise en quarantaine. En particulier, dans le cas de Google, cela s'applique si 5 000 messages ou plus sont envoyés par domaine. Yahoo, d'un autre côté, exige la réussite à la fois du protocole SPF et du protocole DKIM, peu importe le volume de messages envoyé. Une telle politique permet de s'assurer que les courriels provenant de domaines qui échouent les deux vérifications d'authentification sont rejetés ou mis en quarantaine par ces fournisseurs de courrier électronique.

Contrairement à d'autres solutions qui reposent sur un point de défaillance unique, le protocole DMARC emploie une stratégie résiliente couvrant à la fois les côtés source et cible des communications par courriel. Il assure une vérification de sécurité complète de l'information de l'expéditrice ou expéditeur, des détails de la ou du destinataire, de la ligne d'objet, du contenu textuel et d'autres caractéristiques du message.

Tout comme pour SPF et DKIM, le protocole DMARC est facultatif et exige d'être appuyé à la fois par les parties d'expédition et de réception pour une atténuation efficace des risques d'usurpation. Ces protocoles n'offrent pas une protection cryptographique supplémentaire, mais ils assurent l'intégrité du message et l'authenticité de l'expéditrice ou expéditeur.

3 Protection de votre courrier électronique

Toutes les organisations doivent sécuriser leur courrier électronique afin de protéger les données sensibles, y compris les renseignements financiers et l'information nominative. En adoptant les pratiques exemplaires recommandées énumérées dans la présente publication et en investissant dans des outils pour la sécurité du courrier électronique (et au besoin, des services tiers de sécurité des courriels), vous pourrez renforcer la stratégie globale de protection de la confidentialité des données, la sécurité et la résilience de votre organisation.

3.1 Pratiques exemplaires en matière de sécurité pour le courrier électronique

Il est important de mettre en œuvre des stratégies robustes pour protéger vos courriels et empêcher que l'information sensible se trouve entre de mauvaises mains. La présente section explore les pratiques exemplaires essentielles visant à améliorer votre posture de sécurité liée au courrier électronique pour ainsi inspirer la confiance en vos communications par courriel.

3.1.1 Utilisation du chiffrement de courriel et de connexions chiffrées

Le chiffrement des courriels et des connexions joue un rôle important pour assurer une sécurité robuste des messages. Ensemble, ces activités protègent l'information sensible tout au long du processus de communication. Le chiffrement des courriels permet d'assurer la confidentialité du contenu des courriels et prévient les accès non autorisés, même en cas d'interception durant la transmission. Il est particulièrement important de chiffrer les courriels lorsque vous transmettez de l'information sensible ou confidentielle, comme des renseignements financiers, des documents juridiques ou des données personnelles.

Le protocole TLS sert à chiffrer le transport serveur-client et offre une protection seulement si le fournisseur de services de courrier électronique est digne de confiance. Par exemple, si vous avez recours à un fournisseur de services de courrier électronique public, comme Outlook ou Gmail, le protocole TLS assurera la protection des courriels en transit sur Internet, mais le fournisseur de services pourra accéder à tous les courriels une fois qu'ils atteindront ses serveurs. En revanche, les protocoles S/MIME et PGP offrent un chiffrement de bout en bout et permettent d'assurer que le contenu des courriels reste chiffré même lorsque les données résident sur le serveur. Cela offre une couche de sécurité supplémentaire. Les courriels ainsi transmis ne peuvent être lus qu'après un téléchargement de la part de la ou du destinataire sur son appareil, qui devra ensuite entrer sa clé de déchiffrement ou ses justificatifs d'identité ICP. Il est essentiel de savoir que les protocoles S/MIME et PGP offrent l'avantage supplémentaire de protéger les courriels des accès potentiels de la part du fournisseur de services de courrier électronique. Par contraste, le chiffrement TLS ne protège les courriels que lorsqu'ils sont en transit.

Selon la structure de l'organisation, il peut être plus approprié d'utiliser un portail Web protégé par les protocoles TLS/HTTPS pour envoyer et recevoir de l'information sensible. Cette approche offre une méthode plus conviviale pour protéger le transfert de documents importants, plutôt que de compter sur la compréhension et l'application uniforme du chiffrement PGP ou S/MIME des utilisatrices et utilisateurs finaux. Avec un tel système, les données stockées au repos devront être chiffrées, ce qui assurera une sécurité complète pendant tout le cycle de vie. Cette méthode hybride utilise le chiffrement TLS pour une transmission sécurisée sur Internet et un chiffrement dorsal pour le stockage sécurisé afin de mieux équilibrer la convivialité et la robustesse des mesures de sécurité.

3.1.2 Mise en œuvre de protocoles pour valider l'identité des utilisateurs et du serveur

La mise en œuvre de protocoles tels que S/MIME et PGP permet de valider l'identité des utilisatrices et utilisateurs et à s'assurer que l'expéditrice ou expéditeur est bien la personne prétendue. S/MIME et PGP présentent des mécanismes multiusages pour la validation de l'identité des utilisatrices et utilisateurs, la protection contre les infrastructures malveillantes et la protection de la confidentialité du contenu des courriels. En particulier, le protocole S/MIME exploite la confiance envers les autorités de certification (AC) pour la gestion de certificats automatique, tandis que le protocole PGP exploite les relations de confiance directes. Les deux méthodes utilisent le chiffrement et la signature du contenu du courriel, ce qui permet d'éviter les altérations. Les courriels chiffrés peuvent être déchiffrés seulement par la clé privée de la ou du destinataire afin d'assurer l'intégrité du courriel.

Vous devriez également mettre en œuvre la validation de l'identité du serveur (voir les sections 3.4, 3.5, et 3.6 pour plus de détails) dans vos systèmes de courrier électronique, en utilisant des méthodes robustes en plus de compter uniquement sur la simple validation des adresses de courriel ou IP, car ces adresses sont faciles à trafiquer. SPF, DKIM, et DMARC sont des protocoles essentiels qui améliorent la sécurité des courriels. Ils vérifient l'authenticité du serveur d'expédition, assurent l'intégrité du contenu du courriel et fournissent des stratégies pour le traitement des messages qui échouent les vérifications d'authentification.

3.1.3 Sécurité de la passerelle de courrier électronique

Les passerelles de sécurité de courrier électronique sont des points d'inspection pour la détection et le filtrage des maliciels, des pourriels et des tentatives d'hameçonnage. Ces passerelles sont des outils de sécurité essentiels et peuvent être déployées sous différentes formes, comme des appliances matérielles, des instances virtuelles ou des services infonuagiques. Elles fonctionnent à titre de barrières de protection entre le serveur de courrier électronique d'une organisation et l'environnement de courrier électronique externe et inspectent les courriels entrants et sortants. Grâce à un filtrage efficace des menaces, comme les maliciels et les rançongiciels, les passerelles permettent d'améliorer la sécurité globale des courriels. La flexibilité du déploiement de ces passerelles en fait un moyen de protection facile à adapter aux besoins et aux environnements organisationnels divers.

Lors du déploiement d'une passerelle de courrier électronique sécurisée, vous devez prendre en considération le degré de confiance et la fiabilité des fournisseurs tiers. Vous pouvez faire appel à l'expertise et à l'infrastructure de fournisseurs externes qui sont spécialisés en sécurité des courriels. Ces fournisseurs offrent typiquement deux modèles de déploiement pour le filtrage des pourriels et la sécurité des courriels, soit une approche hybride ou une approche entièrement en nuage. Vous devriez évaluer le modèle qui convient le mieux à vos besoins opérationnels et à vos exigences de sécurité.

3.1.4 Création d'une stratégie de sécurité des courriels

Une stratégie de sécurité des courriels représente un guide complet pour la gestion des communications par courriel au sein de votre organisation. Elle couvre les protocoles pour l'utilisation du courrier électronique, le stockage des données, les accès aux appareils et le traitement des menaces de sécurité pour le courrier électronique. Ces protocoles visent tous à protéger l'information sensible et à assurer l'intégrité des canaux de communication. Agissant à titre de cadre stratégique, la stratégie de sécurité des courriels permet non seulement de contrôler les pratiques relatives au courrier électronique, mais elle favorise également une culture de sensibilisation à la sécurité au sein de l'organisation. Grâce à une protection accrue

des données sensibles et des canaux de communication, la stratégie joue un rôle essentiel pour établir une défense résiliente contre les cybermenaces.

3.1.5 Surveillance des activités liées au courrier électronique

Les organisations doivent mettre en œuvre des outils de surveillance pour faire le suivi des activités liées au courrier électronique et détecter les activités atypiques et les comportements suspects. Une surveillance régulière est essentielle pour maintenir la sécurité des systèmes de courrier électronique et repérer les signes potentiels de brèche de sécurité. Une observation constante des activités dans l'environnement de courrier électronique permet aux organisations de détecter les indices d'une compromission.

Une méthode efficace pour améliorer la surveillance des courriels est l'utilisation de systèmes de gestion des informations et des événements de sécurité (GIES). Ces systèmes procèdent à l'agrégation et à l'analyse des données provenant de différentes sources. Ils offrent ainsi des connaissances en temps réel et des alertes pour toute activité suspecte. Grâce aux GIES, vous pouvez repérer les menaces et y répondre rapidement, et ainsi réduire la probabilité de réussite d'une attaque.

Un autre aspect important de la surveillance de la sécurité des courriels est l'examen périodique des rapports DMARC. Ceux-ci offrent des connaissances précieuses à propos de l'utilisation de votre domaine de courrier électronique et des activités malveillantes. De plus, les rapports DMARC présentent de l'information utile sur les sources des courriels qui prétendent provenir de votre domaine, ce qui peut mettre en évidence toute expéditrice ou tout expéditeur non autorisé qui tente de les usurper.

3.1.6 Audits et tests de sécurité des courriels périodiques

Les audits de sécurité des courriels sont essentiels pour évaluer et traiter les vulnérabilités des solutions de sécurité du courrier électronique et assurer la résilience à l'égard des cybermenaces. Ceux-ci exigent des examens périodiques afin d'établir les faiblesses et de mettre en œuvre des améliorations et des mises à jour permettant de renforcer les mesures de sécurité globales des courriels. Les organisations pourront alors apporter des ajustements opportuns et proactifs afin de maintenir un environnement de courriel sécurisé.

3.1.7 Séparation des courriels professionnels et personnels

Séparer les courriels professionnels des courriels personnels aide à protéger les renseignements commerciaux sensibles. L'utilisation d'adresses de courriel professionnelles pour des questions personnelles expose l'organisation à des risques de sécurité et à la compromission potentielle de données confidentielles. De manière similaire, l'utilisation d'adresses de courriel personnelles pour des communications professionnelles expose l'organisation à des risques de sécurité et peut violer les politiques organisationnelles, ainsi que les mesures de sécurité standard.

Afin d'atténuer ces risques de manière efficace, les organisations doivent adopter des politiques claires qui interdisent l'utilisation de comptes de courriel d'entreprise à des fins personnelles ainsi que l'utilisation de comptes personnels à des fins professionnelles. Il est très important de communiquer ces directives à l'ensemble du personnel afin d'assurer une compréhension et une conformité égales à l'échelle de l'organisation.

3.1.8 Vérification des liens dans les courriels avant de cliquer sur ces liens

Vous devez faire preuve de prudence avant de cliquer sur un hyperlien qui se trouve dans un courriel ou de télécharger une pièce jointe, surtout lorsque le courriel provient d'une source inconnue ou suspecte. Prenez le temps de vérifier la légitimité des liens et d'évaluer la crédibilité de l'expéditrice ou expéditeur en vous assurant que le nom de domaine est le bon ou en pointant votre souris sur le lien pour afficher l'adresse réelle. Cette étape simple, mais essentielle, peut vous aider à éviter d'être victime d'attaques par hameçonnage ou de maliciels et à protéger vos renseignements personnels et l'information de votre organisation des risques de sécurité connexes.

3.1.9 Blocage des pourriels et des expéditrices et expéditeurs indésirables

Bloquer les pourriels et les expéditrices et expéditeurs indésirables est une pratique de sécurité du courrier électronique qui vous aidera à atténuer les risques liés aux tentatives d'hameçonnage, à la distribution de maliciel et à d'autres activités malveillantes. Vous pouvez améliorer vos mécanismes de défense en utilisant des outils évolués de filtrage des courriels, qui peuvent notamment analyser le contenu et le comportement de l'expéditrice ou expéditeur. Mettez à jour régulièrement ces filtres pour vous assurer qu'ils sont dotés des renseignements sur les menaces les plus récents et ainsi bloquer les nouvelles techniques de diffusion de courriels indésirables. Personnalisez vos paramètres de sécurité en utilisant des listes d'autorisation et des listes d'exclusion. Les courriels de confiance seront ainsi acceptés, et les messages provenant des expéditrices et expéditeurs figurant sur la liste d'exclusion seront bloqués automatiquement. Par ailleurs, vous devez former les membres du personnel pour qu'ils puissent repérer les caractéristiques courantes des pourriels. Pensez également à examiner périodiquement les courriels qui ont été bloqués pour cerner les faux positifs et signaler les courriels suspects à des fins d'enquête plus approfondie.

3.2 Recommandations en matière de sécurité de l'infrastructure de courrier électronique

Les sections suivantes présentent des recommandations en ce qui a trait à la sécurité de votre infrastructure de courrier électronique.

3.2.1 Serveurs de courrier électronique

Assurez-vous que vos serveurs de courrier électronique sont configurés conformément aux pratiques exemplaires de sécurité, y compris la désactivation des services non utilisés, l'utilisation d'un mécanisme de chiffrement robuste pour les canaux de communication et l'application périodique des correctifs de sécurité. Vous devez également mettre en œuvre des contrôles d'accès robustes afin de limiter les personnes pouvant gérer le serveur de courrier électronique et y accéder. Utilisez l'authentification multifacteur (AMF) pour les accès d'administrateur.

3.2.2 Sécurité des bases de données et du stockage

Chiffrez les données sensibles au repos en utilisant des algorithmes robustes dans le but de fournir une protection contre les accès non autorisés. Appliquez des contrôles d'accès stricts à la base de données et au stockage des courriels et limitez cet accès au personnel autorisé. Examinez périodiquement les autorisations d'accès et apportez des mises à jour, au besoin. Mettez en œuvre des mécanismes de sauvegarde régulière des données de courrier électronique et assurez-vous

que les sauvegardes sont chiffrées et stockées de manière sécurisée. Testez vos procédures de restauration des sauvegardes périodiquement.

3.2.2.1 Contrôles physiques

Sécurisez les accès physiques au serveur qui hébergent l'infrastructure de courrier électronique. Utilisez des mécanismes de contrôle d'accès, comme les lecteurs de biométrie, les badges de sécurité et les systèmes de surveillance. Maintenez des conditions optimales de l'environnement (par exemple, la température et le niveau d'humidité) pour assurer la fiabilité et la longévité du serveur. De plus, assurez-vous que ces systèmes sont sécurisés de façon appropriée.

3.2.3 Considération pour les environnements infonuagiques

Lors de la sélection d'un environnement infonuagique pour vos services de courrier électronique, il est essentiel d'accorder la priorité aux mesures de sécurité offrant une protection efficace de l'information sensible. Vérifiez d'abord que le fournisseur de services de courrier électronique infonuagique sélectionné adhère aux pratiques de sécurité standard de l'industrie. Consultez les certifications, comme SOC 2 et ISO 27001, et examinez avec soin leurs stratégies associées à la protection des données afin de vous assurer qu'elles respectent vos propres normes de sécurité.

Vérifiez que toutes les données transmises et stockées sur le nuage sont chiffrées, à la fois en transit et au repos. Vous devez comprendre les mécanismes de gestion de clés du fournisseur de services infonuagiques et vous assurer que les clés sont protégées adéquatement contre les accès non autorisés.

Utilisez les outils de gestion de l'accès fournis par les services infonuagiques pour mettre en application le principe du droit d'accès minimal. De plus, la mise en œuvre de l'AMF pour les comptes d'administrateur ajoute une couche de sécurité supplémentaire.

Vérifiez périodiquement votre environnement infonuagique pour assurer la conformité aux politiques de sécurité et aux exigences réglementaires de votre organisation. Surveillez tous les changements et incidents qui peuvent avoir des conséquences sur la sécurité des données de vos courriels.

3.3 Pratiques exemplaires en matière de sécurité supplémentaires afin d'améliorer la protection des courriels

Bien que les mesures de sécurité des courriels soient essentielles, le renforcement de la cybersécurité de votre organisation exige une approche complète qui dépasse largement les stratégies qui s'appliquent uniquement au courrier électronique. Dans cette section, nous explorerons d'autres pratiques exemplaires en matière de cybersécurité qui compléteront vos efforts de protection des courriels. La mise en œuvre de ces mesures vous permettra d'améliorer votre posture de sécurité et de protéger vos actifs numériques de différentes menaces.

3.3.1 Phrases de passe ou mots de passe forts et uniques

Créez des phrases de passe ou des mots de passe uniques et forts pour vos comptes. Ne répétez pas et ne réutilisez pas les phrases de passe et les mots de passe pour différents comptes. Il peut aussi être avantageux d'utiliser un gestionnaire de mots de passe pour stocker de manière sécurisée vos phrases de passe et vos mots de passe. Vous devriez créer des phrases de passe et des mots de passe complexes et résilients, car les attaquants exploitent souvent les phrases de passe

et les mots de passe faibles. Pour de plus amples renseignements à propos des pratiques exemplaires relatives aux mots de passe et aux phrases de passe, consultez les documents Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) et Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036).

Pour obtenir des conseils sur l'utilisation de gestionnaires de mots de passe, consultez le document Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025).

3.3.2 Sensibilisation et formation du personnel

La sensibilisation à la sécurité et la formation du personnel sont des composants essentiels à une politique de sécurité efficace pour la sécurité des courriels de l'entreprise. Il est important que les membres du personnel, peu importe le niveau, comprennent la valeur de la protection des données sensibles et les répercussions des attaques et des violations des courriels. Les employées et employés sont la première ligne de défense au sein d'une organisation. Il est donc important de bien les former régulièrement sur le plan de la sécurité afin d'atténuer les risques associés aux erreurs humaines. Plus les membres du personnel sont conscientes et conscients des risques de sécurité liés aux courriels, moins ils seront susceptibles de se faire duper par les tactiques et les attaques des auteurs de menace.

Voici quelques aspects importants à inclure à votre formation :

- les techniques pour repérer et éviter l'hameçonnage, les rançongiciels et les escroqueries par faux ordre de virement;
- les stratégies pour éviter les menaces de sécurité, comme les maliciels, les liens malveillants et les fichiers joints malveillants;
- les moyens d'assurer la sécurité de l'information sensible;
- la classification des données et les procédures de traitement;
- les conseils pour la protection des mots de passe;
- les directives à propos de la réponse à une compromission de compte de courrier électronique et du signalement rapide des courriels suspects et des incidents de sécurité;
- les risques associés à la compromission d'un numéro de téléphone (permutation de module d'identification d'abonné ou de carte SIM);
- les raisons pour lesquelles il est important d'interdire une utilisation combinée des courriels professionnels et personnels;
- les types de fichiers qui conviennent à la transmission de courriels et aux méthodes de transfert de fichiers sécurisé;
- les techniques pour détecter les tentatives de piratage psychologique et connaître ce qu'il ne faut pas transmettre par courriel ou d'autres canaux de communication;
- les politiques de sécurité liées au courrier électronique propres à l'organisation et les réglementations de l'industrie.

L'objectif est d'informer les employées et employés en fournissant des renseignements complets et en améliorant la posture de sécurité générale de l'organisation.

3.3.3 Authentification multifacteur

Utilisez l'authentification multifacteur (AMF) autant que possible pour sécuriser les comptes de courriel. L'AMF permet aussi de prévenir les accès non autorisés aux comptes, même en cas de compromission de mot de passe. Bien que des mots de

passe forts soient utiles, l'AMF ajoute une couche de contrôle d'accès supplémentaire, car un simple mot de passe ne sera pas suffisant pour ouvrir une session. Dans le cadre de l'AMF, les utilisatrices ou utilisateurs doivent fournir deux moyens d'authentification dans le but de vérifier leur identité au cours du processus d'ouverture de session. Les facteurs d'authentification en question peuvent être une combinaison de ce que les utilisatrices et utilisateurs connaissent (par exemple, un mot de passe ou un NIP), de ce qu'ils ont (par exemple, une carte à puce ou une clé de sécurité) ou d'une caractéristique physique (par exemple la biométrie, comme l'empreinte digitale ou la reconnaissance faciale). L'AMF complexifie le travail des auteurs de menace pour obtenir l'accès à vos comptes, plus particulièrement les courriels contenant de l'information sensible.

Une AMF résistante à l'hameçonnage fait référence à des méthodes d'authentification multifacteur conçues pour résister à des attaques par hameçonnage. Ces méthodes ne reposent généralement pas sur des secrets partagés, comme des mots de passe ou des codes, qui peuvent être interceptés ou volés par hameçonnage. Elles utilisent plutôt une authentification cryptographique qui n'expose pas les justificatifs d'identité réutilisables aux fournisseurs de services ou aux attaquants.

Un exemple de technologie AMF résistante à l'hameçonnage est une solution basée sur la norme de sécurité FIDO (*Fast Identity Online*). FIDO utilise des justificatifs d'ouverture de session chiffrés uniques à un site Web et qui ne sont jamais stockés sur un serveur.

Pour en apprendre davantage à propos de l'AMF, lisez les documents Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030) et Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.105).

3.3.4 Mise à jour des logiciels et des systèmes d'exploitation

La mise à jour périodique des logiciels de sécurité des courriels, des logiciels antivirus et des systèmes d'exploitation est importante afin de renforcer la sécurité de vos courriels et de vous protéger contre les vulnérabilités identifiées. Les auteurs de menace misent souvent sur les faiblesses des logiciels désuets afin d'obtenir un accès non autorisé, de voler des données ou d'endommager votre ordinateur. Puisque la plupart des systèmes d'exploitation répandus sont généralement dotés d'un logiciel antivirus intégré, il suffit d'activer les mises à jour automatiques du système et des outils antivirus complémentaires afin de vous assurer d'avoir les correctifs de sécurité les plus récents. Pour en savoir davantage à propos de l'importance des mises à jour, lisez la publication intitulée Application des mises à jour sur les dispositifs (ITSAP.10.096).

3.3.5 Connexion à des réseaux Wi-Fi fiables

Autant que possible, vous devez éviter d'utiliser les réseaux Wi-Fi publics pour les communications par courriel. Ces réseaux sont des cibles attrayantes pour les pirates informatiques, qui tenteront d'obtenir un accès à de l'information sensible ou de voler des données lorsque vous serez en ligne. Si vous devez vous connecter à un Wi-Fi public, faites preuve de précaution afin d'empêcher les auteurs de menace d'intercepter vos données de courrier électronique. Choisissez avec soin le réseau Wi-Fi auquel vous vous connectez. Accordez la priorité aux options de connexion Wi-Fi qui utilisent un chiffrement sécurisé, comme WPA3 (*Wi-Fi Protected Access 3*). Encore mieux, utilisez WPA3 autant que possible conjointement avec le protocole SAE-PK (*Simultaneous Authentication of Equals-Public Key*). Si vous devez accéder à de l'information sensible par courriel, utilisez un réseau privé virtuel (RPV) pour l'établissement d'une connexion sécurisée et la protection des données. Toutefois, il est important de savoir que les services RPV n'offrent pas tous le même niveau de confiance. Choisissez un RPV fourni par

une organisation de confiance, plutôt que d'utiliser des services de RPV offerts au public. Pour de plus amples renseignements à propos de la sécurité des réseaux Wi-Fi, lisez les documents La sécurité du Wi-Fi (ITSP.80.002) et Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009).

3.3.6 Création d'un plan d'intervention en cas d'incident

Les organisations doivent créer un plan d'intervention en cas d'incident et le mettre à jour périodiquement. Le plan en question devrait inclure une réponse en cas d'incident de sécurité des courriels. Ce plan doit indiquer les mesures particulières à entreprendre dans l'éventualité d'un incident de sécurité, ce qui comprend l'isolation des systèmes affectés dans le but de prévenir les dommages supplémentaires, l'identification et l'atténuation des vulnérabilités qui ont été potentiellement exploitées ainsi que le signalement aux parties prenantes pertinentes, comme les équipes de TI, la direction et possiblement même les utilisatrices et utilisateurs touchés. Pour plus d'information sur la création d'un plan de réponse en cas d'incident, consultez Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003).

3.3.7 Sauvegarde des fichiers importants

Vous devez assurer la sécurité et la disponibilité de vos courriels en procédant à une sauvegarde périodique. Ainsi, vous serez protégée ou protégé contre les suppressions accidentelles, les défaillances matérielles et les brèches de sécurité. Pour ce faire, explorez les solutions de sauvegarde dans le nuage, de sauvegardes locales ou d'autres solutions isolées, selon ce qui convient le mieux aux besoins de votre organisation. Pensez à sauvegarder les fichiers critiques à plus d'un endroit et à utiliser des systèmes de sauvegarde isolés, qui ne sont pas connectés au réseau principal. Cette précaution permettra d'éviter les attaques par rançongiciel et de limiter la propagation des autres maliciels sur l'infrastructure de sauvegarde. Menez régulièrement des exercices de restauration afin de vérifier l'intégrité et l'efficacité de vos systèmes de sauvegarde. Cette pratique permettra de relever les problèmes potentiels liés au processus de sauvegarde et assurera une reprise en douceur dans l'éventualité d'une cyberattaque. Pour des conseils à propos des sauvegardes de fichiers, lisez la publication Sauvegarder et récupérer vos données (ITSAP.40.002).

3.4 Recours à des spécialistes de la sécurité des courriels

Les organisations qui souhaitent une protection évoluée de leurs courriels, ou celles qui ne disposent pas d'une expertise interne, devraient recourir à des spécialistes de la sécurité des courriels ou à une solution infonuagique appropriée.
Les fournisseurs de services tiers de sécurité des courriels peuvent offrir une solution de défense à plusieurs couches avec des renseignements avancés sur les menaces, des options de filtres robustes, une surveillance en temps réel, une détection proactive des menaces et des capacités de réponse rapide. Ces services peuvent inclure des analyses et des rapports détaillés qui appuieront les efforts de conformité, identifieront les vulnérabilités et fourniront des renseignements à propos des menaces de sécurité courantes s'appliquant aux courriels. Pour certaines organisations, l'externalisation peut permettre d'optimiser l'attribution des ressources, de réduire le fardeau associé qui pèse sur les équipes internes et d'assurer une défense complète contre les cybermenaces.

Pour vous assurer que les fournisseurs de service tiers de sécurité des courriels protègent adéquatement vos courriels et l'information sensible, vous devez tout d'abord appliquer une analyse d'intégrité de la chaîne d'approvisionnement. Une telle analyse comprend des mécanismes rigoureux d'évaluation et de diligence raisonnable concernant les pratiques de sécurité du fournisseur, son infrastructure et son respect des normes et des réglementations de l'industrie. Par exemple, vous devez

vérifier les antécédents du fournisseur, ses certifications ainsi que tous les audits ou toutes les évaluations de sécurité informatique pertinents. Vous pourrez ainsi vous assurer que le fournisseur de services tiers saura protéger adéquatement vos données, ce qui réduira les risques associés à l'externalisation des services. Pour de plus amples renseignements à propos de l'intégrité de la chaîne d'approvisionnement, lisez les publications intitulées La cybersécurité et la chaîne d'approvisionnement : évaluation des risques (ITSAP.10.070) et Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels (ITSM.10.071).

Vous trouverez ci-dessous une liste des différents types de services de sécurité des courriels à prendre en considération.

3.4.1 Détonation et mise en bac à sable d'un courriel

Dans le contexte de la sécurité des courriels, la détonation correspond à l'exécution d'un fichier joint ou d'un lien dans un courriel potentiellement malveillant dans un environnement contrôlé afin d'en analyser le comportement et de déterminer s'il s'agit en effet d'une menace. Ce processus, que l'on nomme également la mise en bac à sable, se déroule dans un environnement sécurisé et isolé et permet aux spécialistes de la sécurité d'examiner soigneusement les fichiers suspects, sans risque de porter atteinte au réseau ou aux systèmes de l'organisation. En observant les actions du fichier joint dans un environnement contrôlé, les équipes de sécurité peuvent recueillir des renseignements utiles dans le but de mieux comprendre et d'atténuer les risques de sécurité.

3.4.2 Contrôle du contenu

Le contrôle du contenu dans les services de sécurité des courriels consiste à utiliser des technologies évoluées, comme l'IA et l'apprentissage automatique, pour analyser le contenu des courriels et détecter les éléments non sécuritaires. Ces services peuvent ainsi repérer et bloquer différents types de contenu potentiellement malveillant. En particulier, les capacités de contrôle vérifient et scrutent les images et le contenu joints ou intégrés aux courriels. Grâce à l'IA et à l'apprentissage automatique, ces services peuvent détecter les maliciels dans les images et le contenu, et prévenir les téléchargements et les exécutions connexes.

Des filtres sont conçus pour détecter automatiquement les pourriels et les cas d'hameçonnage, ainsi que pour bloquer les courriels malveillants potentiels. Les services offerts par des tiers améliorent la détection des pourriels et de l'hameçonnage grâce à l'utilisation d'algorithmes évolués et de renseignements sur les menaces. Ainsi, les fournisseurs peuvent analyser le contenu du courriel et le comportement de l'expéditrice ou expéditeur dans le but de cerner les tentatives d'hameçonnage et de les bloquer avant qu'elles atteignent les boîtes de réception des utilisatrices et utilisateurs. Ces filtres bloquent également les courriels contenant des fichiers joints qui tentent d'accéder aux registres du système ou aux dossiers sensibles, ou encore qui essaient de communiquer avec des adresses IP externes ou de télécharger des fichiers à partir de sources externes. En général, ces mesures contribuent à une défense robuste contre les pourriels, l'hameçonnage et les menaces de sécurité dans les communications par courriel.

En plus de l'utilisation de l'IA, de l'apprentissage automatique et des filtres de pourriel et d'hameçonnage, vous disposez d'autres méthodes traditionnelles afin de filtrer de manière efficace le contenu des courriels et de bloquer ou de mettre en quarantaine les fichiers joints ou d'autres types de fichier suspects :

- utiliser les fonctionnalités du serveur de courrier électronique afin de bloquer ou de mettre en quarantaine les fichiers joints ou les types de fichier suspects;

- mettre en œuvre des listes d'autorisation qui autorisent seulement les types de fichiers sécuritaires, ce qui renforce la sécurité;
- convertir automatiquement les documents MS Office ou d'autres types de documents qui contiennent des macros en formats plus sécuritaires, comme PDF, dans le but d'atténuer les risques associés aux macros malveillantes;
- retirer ou désactiver le contenu actif afin d'éviter l'exploitation;
- déployer des logiciels antivirus et antimaliciel permettant d'analyser les fichiers joints, y compris les fichiers d'archives Zip, Rar et 7zip (qui pourraient être mis en quarantaine ou supprimés s'ils sont chiffrés);
- désactiver les macros des documents MS Office, car les macros sont un vecteur d'attaque courant.

3.4.3 Systèmes d'authentification

Les systèmes d'authentification sont essentiels pour fournir une défense contre les courriels trafiqués et permettent d'assurer la légitimité des expéditrices et expéditeurs, ainsi que d'atténuer diverses cybermenaces.

Les outils anti-usurpation utilisent les protocoles d'authentification dans le but de prévenir les attaques par usurpation d'identité et détectent ou rejettent les messages suspects. Des services tiers peuvent aider les organisations pour la mise en œuvre et la gestion des protocoles d'authentification, comme SPF, DKIM et DMARC. L'objectif principal est de prévenir l'usurpation de domaine, de détecter ou de rejeter les messages suspects et de garantir l'authenticité de la communication par courriel afin de réduire les risques de cybermenace.

3.4.4 Chiffrement des courriels

Le chiffrement des courriels est une mesure de sécurité qui emploie des techniques de chiffrement afin d'atténuer de manière efficace les risques associés à l'interception des courriels. Les courriels chiffrés ne peuvent être lus que par les expéditrices et expéditeurs et les destinataires autorisés, ce qui joue un rôle important dans la prévention des accès non autorisés et de l'interception d'information sensible.

Les fournisseurs de services de sécurité des courriels offrent des solutions de chiffrement de courriel robustes qui améliorent la sécurité de l'information sensible lors de la transmission. De telles solutions intègrent une grande variété de protocoles et des méthodes de chiffrement évoluées de type pousser-tirer. Avec un chiffrement de type pousser, les courriels sont convertis en fichiers chiffrés et sont joints à un autre courriel, ce qui assure une transmission sécurisée et restreint l'accès des destinataires non autorisés. Un chiffrement de type tirer offre une récupération de courriel sécurisée à partir d'un portail désigné, ce qui permet l'accès uniquement aux personnes dotées des justificatifs d'identité appropriés. Ces mesures, ensemble, protègent vos courriels des accès non autorisés et assurent la confidentialité de vos communications.

3.4.5 Passerelles de sécurité de courrier électronique

Les passerelles de sécurité de courrier électronique sont un autre service offert par les spécialistes en matière de sécurité des courriels. Grâce au déploiement de ces passerelles, les spécialistes peuvent garantir que tous les courriels entrants et sortants sont soigneusement inspectés, que le contenu malveillant est bloqué et que vos canaux de communication sont protégés.

3.4.6 Surveillance continue

Il existe des services de sécurité des courriels qui surveillent continuellement les communications et qui recueillent des renseignements sur les menaces afin de fournir une défense contre les menaces et les vulnérabilités émergentes. Ces services surveillent activement l'environnement des courriels, détectent les nouveaux vecteurs d'attaque et s'adaptent rapidement à l'évolution des risques. En utilisant les renseignements sur les menaces, ces services sont en mesure d'offrir une protection rapide et efficace contre les cybermenaces émergentes.

3.4.7 Production de rapports et d'analyses

Les outils de sécurité des courriels offrant des options de production de rapports et d'analyses incluent également des fonctions de surveillance du trafic de courrier électronique et de suivi des incidents de sécurité. Grâce à ces capacités, les organisations peuvent obtenir des données précieuses à propos des menaces pour la sécurité et agir de manière proactive afin de répondre aux vulnérabilités. Ces outils produisent des rapports détaillés fournissant une vue globale du contexte de la sécurité des courriels et aident ainsi les organisations à déterminer les schémas, les tendances et les secteurs qui méritent une attention accrue.

4 Résumé

Il est important que votre organisation assure la protection des courriels contenant des données sensibles, y compris les données financières, l'information exclusive et les renseignements à propos de la clientèle et du personnel. Pour ce faire, il est important de mettre en œuvre des pratiques exemplaires en matière de sécurité des courriels, y compris le chiffrement, l'authentification, les passerelles de sécurité, la surveillance et les audits périodiques. L'adoption de telles pratiques permet non seulement d'assurer une défense robuste contre les violations potentielles, mais également de protéger la confidentialité de l'information sensible lors de la transmission des courriels.

Les protocoles de sécurité des courriels, y compris TLS, S/MIME, SPF, DKIM et DMARC, jouent un rôle essentiel pour le renforcement de la sécurité des communications par courriel. Ces protocoles permettent de répondre à différents aspects de cybersécurité, comme le chiffrement, l'authentification, la protection contre l'hameçonnage et le désamorçage des tentatives d'usurpation.

L'application de ces protocoles de sécurité et des pratiques exemplaires énoncées dans le présent document aideront votre organisation à établir un environnement de communication de confiance, surtout pour les transactions impliquant des données sensibles. Ensemble, ces moyens permettront de renforcer la stratégie générale de confidentialité des données, la posture de sécurité et la résilience de votre organisation. En priorisant la sécurité des courriels, les organisations inspirent la confiance aux parties prenantes, tout en favorisant une culture de sensibilisation à la cybersécurité et une démarche proactive face aux cybermenaces émergentes.