ASSOCIATION

MESURES ANTI-HAMEÇONNAGE:

RECOMMANDATION SECTORIELLE POUR LES FOURNISSEURS DE SERVICES DE COURRIER ÉLECTRONIQUE

De quoi s'agit-il?

Les e-mails d'hameçonnage constituent une porte d'entrée majeure pour les cyberattaques croissantes auxquelles sont exposées les entreprises et les particuliers en Suisse. Les fournisseurs de services de courrier électronique sont en première ligne pour répondre aux préoccupations des clientes et clients concernant les e-mails d'hameçonnage. Les attaques d'hameçonnage contribuent à alourdir la charge de travail de ces fournisseurs de services. De plus, elles peuvent occasionner des dommages considérables aux clientes et clients. Pourtant, identifier les attaquants et intenter des actions en justice à leur encontre reste difficile dans la pratique.[1]

La présente recommandation sectorielle de Swico présente les mesures concrètes et standardisées prises par les fournisseurs de services de courrier électronique suisses contre les e-mails d'hameçonnage. Soutenue par l'Association Suisse des Télécommunications, le Centre National pour la Cybersécurité NCSC, l'Alliance Suisse pour la Sécurité sur Internet SISA et SWITCH, son objectif est de permettre aux fournisseurs de renforcer la protection de leurs clientes et clients contre les e-mails d'hameçonnage et d'aider les autorités compétentes à identifier et à poursuivre les attaquants.

Avec les mesures recommandées, Swico suit les règles applicables du droit suisse en matière de filtrage et de suppression des courriers indésirables non autorisés et de mise à disposition d'informations aux autorités et aux tribunaux. En outre, ces mesures exploitent la marge de manœuvre juridique pour présenter des recommandations concrètes sur le comportement à adopter afin de détecter et de prévenir les tentatives d'hameçonnage et d'informer les clientes et clients des mesures prises ou possibles. Cette recommandation sectorielle a pour but d'orienter les fournisseurs dans l'évaluation des mesures possibles et appropriées à prendre pour faire face aux cyberattaques menées par le biais des e-mails d'hameçonnage.

A. Besoin et objectif

1 Le phénomène de l'hameçonnage

Le «phishing», ou hameçonnage, est la contraction des mots anglais «password» (mot de passe), «to harvest» (récolter) et «to fish» (pêcher). Il désigne la pratique visant à tenter d'obtenir des données sensibles, telles que des mots de passe ou des informations de cartes de crédit, par le biais de faux e-mails, SMS ou sites Web. Cette recommandation sectorielle se limite à l'outil d'attaque le plus répandu: l'e-mail. Dans un e-mail d'hameçonnage, l'expéditeur propose généralement une offre alléchante ou exerce une pression sur le destinataire pour l'inciter à remplir un faux formulaire, à cliquer sur un lien renvoyant vers une fausse page Web ou à ouvrir une pièce jointe infectée. Cette pratique est également appelée «ingénierie sociale».

2 Une protection juridique contre les courriers indésirables insuffisante

La législation en vigueur interdit les courriers indésirables et donc, au moins indirectement, les e-mails d'hameçonnage envoyés en masse. Les courriers indésirables sont considérés comme de la «publicité de masse déloyale» (art. 3, let. o de la loi fédérale contre la concurrence déloyale, LCD, en liaison avec l'art. 45a de la loi sur les télécommunications, LTC). Les fournisseurs sont tenus de protéger leurs clientes et clients contre la réception de courriers indésirables par des mesures techniquement réalisables (art. 83, al. 1 de l'ordonnance sur les services de

[1] Voir à ce sujet: iBarry, Phishing: L'e-mail avec l'appât, consulté le 11 mars 2021, disponible sur https://www.ibarry.ch/fr/risques-sur-internet/phishing/.

Swico
Lagerstrasse 33
CH-8004 Zurich

Tél. +41 44 446 90 90
www.swico.ch
info@swico.ch

télécommunication, OST, SR 784.101.1), autrement dit par la mise en place de filtres anti-spam. Les fournisseurs sont par ailleurs autorisés à supprimer les messages correspondants (art. 83, al. 2, OST).

Cependant, les e-mails d'hameçonnage ne sont pas toujours des e-mails envoyés en masse. Il arrive de plus en plus souvent que les attaquants tentent d'induire en erreur les membres d'une organisation donnée en s'adressant à eux de manière ciblée et en usurpant l'identité d'une personne connue du destinataire, comme un supérieur hiérarchique. S'il est indéniable que les attaquants commettent des infractions (escroquerie, utilisation frauduleuse d'un système de traitement de données et collecte non autorisée de données, pour l'essentiel), les moyens de poursuite pénale existants sont inefficaces contre les auteurs de ces attaques, qui agissent de façon anonyme, le plus souvent depuis l'étranger. Néanmoins, la législation en vigueur offre aux fournisseurs la marge de manœuvre nécessaire pour leur permettre de prendre des mesures contre les attaques d'hameçonnage et atténuer ainsi les risques pour leurs clientes et clients.

3 Objectifs des mesures

Afin de prévenir tout dommage et d'éviter aux fournisseurs des frais de support élevés, les clientes et clients doivent éviter toute interaction avec les e-mails d'hameçonnage. L'utilisation de filtres ainsi que la suppression ou l'élimination des messages d'hameçonnage peuvent s'avérer utiles à cet effet.

L'échange d'informations entre les fournisseurs et les autorités concernées – en particulier les autorités de poursuite pénale et le Centre national pour la cybersécurité (NCSC) – doit être amélioré. De cette manière, les fournisseurs espèrent pouvoir aider les autorités dans l'identification et la poursuite des cyberattaquants et contribuer à l'amélioration des bases de données utilisées pour les filtres.

Les fournisseurs doivent sensibiliser leurs clientes et clients et leur apprendre à détecter ces e-mails d'hameçonnage afin de les aider à éviter d'éventuels dommages pour eux-mêmes ou pour des tiers, d'une part, et des frais de support élevés pour les fournisseurs, d'autre part.

Les clientes et clients doivent être informés de manière transparente sur les mesures de protection prises par les fournisseurs contre les e-mails d'hameçonnage. Les mesures de sensibilisation et d'information, tout comme les contrats et les CGV applicables aux clientes et clients, servent également cet objectif.

B. Mesures

1 Protection directe des clientes et clients contre les e-mails d'hameçonnage

a) Utilisation de filtres pour l'identification des e-mails d'hameçonnage

Cadre juridique:
La recherche d'e-mails à l'aide de filtres conformes à l'état de la technique en vue d'empêcher les courriers indésirables est explicitement autorisée en Suisse et constitue même une obligation pour les fournisseurs de services de télécommunication. Les filtres anti-spam doivent être déployés afin de pouvoir identifier les e-mails d'hameçonnage envoyés en masse.

La recherche d'e-mails est soumise au secret des télécommunications de l'expéditeur et du destinataire, à condition que ce dernier n'ait pas ouvert sa boîte de réception. Les e-mails, en tant qu'«envois non verrouillés», peuvent faire l'objet d'une recherche par le fournisseur si la prévention des menaces pour la cliente ou le client et les tiers justifie une telle mesure. Des filtres peuvent donc être déployés et appliqués sur la base juridique existante pour les e-mails d'hameçonnage considérés comme courriers indésirables.

Les données personnelles des personnes concernées (c.-à-d. les destinataires et les victimes potentielles) sont soumises à la législation sur la protection des données. L'utilisation de ces filtres doit donc être signalée aux clientes et clients dans les contrats. Les filtres anti-hameçonnage doivent utiliser le moins de données personnelles possible. Les échantillons nécessaires aux filtres doivent être élaborés sur la base de données anonymisées ou au moins pseudonymisées. L'utilisation des adresses IP des serveurs à partir desquels les e-mails d'hameçonnage sont envoyés est nécessaire pour le filtrage. Celles-ci permettent la création d'une liste de blocage basée sur

le DNS («DNSRBL»). Les DNSRBL peuvent exploiter d'autres attributs pertinents, telles que les domaines d'hameçonnage connus ou les adresses e-mail d'expéditeurs compromis. L'utilisation d'attributs d'en-tête d'e-mail est également autorisée si ces derniers ne permettent pas de déduire directement l'identité d'une personne.

Les dispositions contractuelles qui lient les fournisseurs aux clientes et clients assurent une transparence, évitent les malentendus du côté des clientes et clients et renforcent la sécurité juridique. L'ajout d'une disposition correspondante dans le contrat ou les CGV est donc recommandé.
Le recours éventuel à des tiers en tant que prestataires de services doit être spécifié par écrit afin de veiller à ce que ces tiers respectent les mêmes limites que les fournisseurs lors du traitement éventuel de données personnelles.

Mise en œuvre technique:

- L'utilisation de DNSRBL, ou Real-Time-Block-Lists («RBL»), est recommandée. Le choix et l'utilisation de ces listes doivent être contrôlés en amont et de manière régulière.
- Les e-mails provenant de noms de domaine inexistants doivent être rejetés, même si le nom de domaine inexistant est utilisé dans le champ «De».
- Les e-mails contenant des URL de sites d'hameçonnage connus selon le flux SISA doivent également être rejetés.

b) Suppression des e-mails d'hameçonnage

Cadre juridique:
Les e-mails qui n'ont pas encore été délivrés sont soumis au secret des télécommunications. Les fournisseurs sont autorisés à supprimer les e-mails d'hameçonnage envoyés en masse afin que les clientes et clients ne les reçoivent pas. Le fournisseur est même tenu de proposer aux clientes et clients des mesures techniques afin de les protéger contre les courriers indésirables. Les e-mails qui constituent une «publicité de masse déloyale» (courrier indésirable) peuvent être supprimés par le fournisseur de services de télécommunication s'ils n'ont pas encore été livrés dans la boîte de réception des clientes et clients.

Par ailleurs, il est recommandé aux fournisseurs d'informer les clientes et clients au sujet de la possibilité de suppression des e-mails d'hameçonnage et d'ajouter une disposition correspondante dans les contrats ou CGV applicables.

Mise en œuvre technique:
Lorsque cela est possible, les messages identifiés comme des e-mails d'hameçonnage sont directement rejetés par le serveur de messagerie destinataire le plus éloigné pendant la connexion, dans le respect des directives RFC.

Si cela n'est pas possible, les e-mails sont alors déplacés dans un dossier distinct prévu à cet effet (dossier SPAM, par exemple) du compte de messagerie de la cliente ou du client au lieu d'être livrés dans sa boîte de réception.

c) Élimination des e-mails d'hameçonnage

Cadre juridique:
Si des e-mails d'hameçonnage ont déjà été livrés dans la boîte de réception de la cliente ou du client, mais que celle-ci ou celui-ci ne les a pas encore ouverts, le secret des télécommunications s'applique à l'élimination/au déplacement de ces e-mails. Une divulgation à des tiers apparaîtrait dès lors comme problématique dans la mesure où, par exemple, les conditions permettant une surveillance ne seraient pas réunies dans le cadre d'une procédure pénale. Le secret des télécommunications ne s'oppose pas à l'utilisation de filtres anti-hameçonnage dans le but de protéger les clientes et clients contre les e-mails d'hameçonnage. Toutefois, dès que les clientes et clients sont en mesure de décider eux-mêmes de l'action à effectuer sur les e-mails reçus après avoir ouvert leur boîte de réception, le secret des télécommunications ne s'applique plus.

Il est recommandé de prévoir des dispositions contractuelles sur la distribution et la conservation des e-mails dans la boîte de réception et sur le serveur, ainsi que sur l'analyse et le déplacement des messages de la boîte de réception. Celles-ci permettent de minimiser le risque résiduel de violation du secret des télécommunications à

l'encontre des clientes et clients et de faire face à toute surprise éventuelle pour éviter une perte de confiance des clientes et clients à l'égard du fournisseur.

Les données personnelles présentes sur le serveur du fournisseur sont soumises à la législation sur la protection des données. Les données personnelles étant, en règle générale, également concernées par le filtrage et l'élimination, les clientes et clients doivent être informés de manière transparente sur de telles mesures, y compris du point de vue de la protection des données (au moins dans les CGV, dans une déclaration de confidentialité ou dans une autre section des documents contractuels correspondants).

Le recours éventuel à des tiers en tant que prestataires de services doit être spécifié par écrit afin de veiller à ce que ces tiers respectent les mêmes limites que les fournisseurs lors du traitement éventuel de données personnelles.

Mise en œuvre technique:
Les messages identifiés comme des e-mails d'hameçonnage peuvent être déplacés par défaut de la boîte de réception des clientes et clients vers un dossier distinct prévu à cet effet (dossier SPAM, par exemple).

d) Utilisation de normes pour la sécurité des e-mails

Mise en œuvre technique:
Les normes existantes visant à réduire l'utilisation abusive des e-mails (p. ex. Sender Policy Framework «SPF», Domain-based Message Authentication, Reporting and Conformance «DMARC» et DomainKeys Identified Mail «DKIM») doivent être mises en œuvre lors de l'envoi et de la réception d'e-mails. Les normes SPF, DKIM et DMARC doivent notamment être utilisées pour les e-mails entrants et filtrées sur la base de la politique publiée par le propriétaire du domaine.

Il est recommandé aux fournisseurs de tenir compte des bonnes pratiques du Messaging Malware Mobile Anti-Abuse Working Group («M3AAWG»). Celles-ci comprennent des mesures pour l'envoi, le filtrage à la réception et la protection de l'infrastructure de messagerie (https://www.m3aawg.org/published-documents).

e) Communication auprès de la clientèle et dispositions contractuelles

Les clientes et clients doivent être informés des mesures de filtrage, de suppression et d'élimination des e-mails d'hameçonnage. Il est recommandé de prévoir des dispositions correspondantes dans les contrats ou les CGV (voir le texte type au point 4 ci-dessous).

2 Coordination avec les autres fournisseurs et les autorités

a) Signalement des tentatives d'hameçonnage

Cadre juridique:
Les fournisseurs peuvent fournir aux autorités compétentes des informations sur les tentatives d'hameçonnage détectées afin de faciliter le suivi des campagnes d'hameçonnage.

Les données personnelles des destinataires d'e-mails d'hameçonnage doivent être anonymisées avant d'être transmises lorsque cela est possible, à condition qu'une telle mesure n'empêche pas le suivi des campagnes d'hameçonnage.

Les clientes et clients doivent être informés de manière transparente sur le fait que des e-mails peuvent être transmis par les fournisseurs. Par ailleurs, les fournisseurs doivent avertir les clientes et clients sur la possibilité qui leur est laissée de signaler eux-mêmes des URL d'hameçonnage via antiphishing.ch ou une adresse de signalement mise à disposition par le fournisseur.

Mise en œuvre technique:
Les fournisseurs transmettent au NCSC les e-mails d'hameçonnage via reports@antiphishing.ch et/ou signalent les URL d'hameçonnage détectées via antiphishing.ch (ou une API correspondante).

b) Implémentation et contribution aux bases de données de filtrage

Cadre juridique:
Les fournisseurs peuvent échanger entre eux et avec les autorités compétentes des informations sur les tentatives d'hameçonnage détectées, y compris de manière automatisée.

Les données des destinataires d'e-mails d'hameçonnage doivent être anonymisées, dans la mesure du possible.

Les clientes et clients doivent être informés de manière transparente sur les filtres et l'amélioration de ces derniers permise par l'échange de données.

Mise en œuvre technique:
Il est recommandé aux fournisseurs d'utiliser la liste de blocage gérée par Swiss Internet Security Alliance (SISA) à l'adresse https://fuchur.switch.ch et d'y contribuer (en communiquant l'API correspondante, le cas échéant).

3 Sensibilisation de la clientèle

Les fournisseurs doivent attirer l'attention des clientes et clients sur le risque lié aux e-mails d'hameçonnage par l'intermédiaire de canaux adaptés (p. ex. leur propre site Web, un message dans le panneau de contrôle) et leur recommander des mesures pour se protéger contre les cyberattaques menées par le biais des e-mails d'hameçonnage. Afin de garantir une communication aussi uniforme et exhaustive que possible aux clientes et clients, il est recommandé de leur signaler l'existence des ressources suivantes et de leur fournir les liens associés:

- ibarry.ch de la SISA, à l'adresse https://www.ibarry.ch/fr/risques-sur-internet/phishing/;
- Prévention Suisse de la Criminalité (PSC), à l'adresse https://www.skppsc.ch/fr/sujets/internet/phishing/ et https://www.skppsc.ch/fr/wp-content/uploads/sites/5/2018/10/phising_fr_web.pdf.

Il est recommandé aux clientes et clients d'utiliser les options de signalement des e-mails d'hameçonnage via reports@antiphishing.ch et des URL d'hameçonnage via antiphishing.ch afin de contribuer à la détection et la prévention des e-mails d'hameçonnage.

4 Ajout d'une disposition aux contrats et CGV

Disposition relative aux mesures anti-hameçonnage dans les CGV:
«Nous attachons une grande importance à protéger nos clientes et clients contre les éventuels dommages occasionnés par les courriers indésirables (y compris les e-mails d'hameçonnage, voir [lien vers la page d'information du fournisseur]). Pour ce faire, nous mettons en place des mesures techniques, telles que l'utilisation de filtres, en vue d'identifier et d'intercepter les e-mails suspects. En supprimant ou en déplaçant les e-mails suspects, nous atténuons les risques pour nos clientes et clients. Nous pouvons également appliquer de telles mesures aux e-mails présents dans votre boîte de réception qui ont été identifiés rétrospectivement comme des e-mails d'hameçonnage. Nous pouvons également avoir recours à des sources d'information externes appropriées afin d'améliorer la détection des e-mails d'hameçonnage. À cet égard, nous mettons en application la recommandation sectorielle de l'association faîtière Swico concernant les e-mails d'hameçonnage.

Pour veiller à ce que nos mesures soient encore plus efficaces et que les auteurs des tentatives d'hameçonnage puissent faire l'objet de poursuites judiciaires, nous nous réservons le droit de signaler les e-mails d'hameçonnage détectés aux autorités et organisations compétentes (p. ex. au NCSC via antiphishing.ch). Nous pouvons notamment transmettre à des tiers (p. ex. à la SISA, au NCSC ou aux autorités de poursuite pénale suisses) les URL suspectes, les adresses IP du serveur d'un expéditeur ainsi que les attributs d'en-tête d'e-mail pertinents en vue d'améliorer les mesures de filtrage et à des fins de poursuite pénale. Nous veillons autant que possible à ne pas divulguer de données personnelles. Les informations transmises peuvent, dans des cas exceptionnels, inclure des données personnelles, telles que des noms, des adresses e-mail et le contenu d'e-mails à caractère personnel. Toutefois, les données personnelles ne peuvent être utilisées par leurs destinataires qu'à des fins d'identification et de suivi des tentatives d'hameçonnage, ou pour lutter contre ces dernières.

Les mesures techniques anti-hameçonnage ne sont pas exemptes d'erreurs et peuvent classer à tort des e-mails comme suspects («faux positifs») ou ne pas détecter certains e-mails d'hameçonnage («faux négatifs»). Nous excluons toute responsabilité pour les dommages occasionnés ou la perte de données en lien avec les mesures anti-hameçonnage, sauf si une négligence grave ou un acte intentionnel de notre part a entraîné un tel dommage.»

Pour toute question concernant la Recommandation sectorielle sur les mesures anti-hameçonnage:

Giancarlo Palmisani
SWICO
Responsable des prestations de l'association
Mobile: +41 79 429 53 39 Direct: +41 44 446 90 85
E-mail: Giancarlo.palmisani@swico.ch