privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Check-list
Déchiffrement de connexions web encryptées

1 Introduction

Les connexions web encryptées (connexions https) font partie du standard dans l'Internet. Elles constituent une mesure technique centrale pour garantir la sphère privée et la sécurité de l'information dans la consultation de sites web, selon les dispositions sur la sécurité de l'information dans les lois cantonales sur (l'information et) la protection des données. Les connexions encryptées limitent pourtant les mesures de protection, comme le filtrage des malwares ou des contenus indésirables. C'est pourquoi il y a souvent un intérêt à ce qu'elles puissent être déchiffrées par les serveurs proxy web ou autres applications semblables.

Le déchiffrement ne touche pas seulement à la sphère privée des personnes concernées, mais aussi à l'intégrité et à l'authenticité des transactions en ligne. Une analyse des risques ainsi que des mesures conformes à la protection des données sont impératives lors de la mise en œuvre.

Cet aide-mémoire soutient les organes publics en charge du déchiffrement ainsi que les services internes ou externes qui mettent en œuvre les mesures de déchiffrement de connexions web encryptées conformément à la protection des données.

2 Check-list:

Est-il possible de déchiffrer les connexions web encryptées conformément à la protection des données?

2.1 Une analyse et évaluation des risques a-t-elle été effectuée ?

Oui → aller à la question 2.2

Non → déchiffrement non admissible

- Il doit être démontré que les mesures de réduction des risques justifient **la rupture** d'une connexion SSL.

2.2 La transparence du déchiffrement est-elle garantie?

Oui → aller à la question 2.3.

Non → déchiffrement non admissible

V1.0 / 28.04.2020

privatim
c/o Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 205, CH-4010 Basel
Tel. +41 (61) 201 16 40
praesident@privatim.ch, www.privatim.ch

- Le but du déchiffrement ainsi que la base légale nécessaire doivent être clairement documentés.
- Il faut régler dans quels cas les connexions sont déchiffrées.
- Les utilisatrices et utilisateurs doivent être informés des risques liés au déchiffrement avant le déchiffrement de la connexion.
- Les informations nécessaires quant au déchiffrement des connexions doivent être mises à disposition des utilisatrices et utilisateurs sur le site web. Le site web doit documenter les processus et les déroulements.
- Les utilisatrices et utilisateurs doivent être informés de la façon de pouvoir reconnaître si le certificat provient du site web qu'ils consultent.
- Les erreurs et problèmes en lien avec le certificat doivent être transmis correctement au niveau technique au browser client. Les utilisatrices et utilisateurs doivent être informés de manière transparente au moyen de messages d'erreurs.

2.3 Une procédure pour les exceptions existe-t-elle?

Oui → aller à la question 2.4

Non → déchiffrement non admissible

- Il faut implémenter un processus qui permet aux utilisatrices et utilisateurs de demander une exception au déchiffrement de connexions pour accéder aux sites web. Avant de décider d'accepter ou non une exception, il faut effectuer une pondération des intérêts et la demandeuse ou le demandeur doit être informé de la décision.

2.4 Une chaîne de certificats valable et de confiance est-elle utilisée?

Oui → aller à la question 2.5

Non → déchiffrement non admissible

- Un certificat valide doit être préparé à l'attention de l'organe public responsable du déchiffrement des connexions.
- Si un site web utilise un certificat périmé (expired), les utilisatrices et utilisateurs doivent en être informés. Ils doivent avoir la possibilité de consulter le site web ou non.
- Si un site web consulté utilise un certificat d'une autorité de certification (CA) qui n'est pas digne de confiance, les utilisatrices et utilisateurs doivent en être informés. Ils doivent avoir la possibilité de consulter le site web ou non.
- Si un site web consulté utilise un certificat révoqué (revoked), la connexion doit être bloquée et les utilisatrices et utilisateurs doivent en être informés.
- La durée de validité du certificat généré pour le déchiffrement doit être plus courte ou égale à celle du certificat d'origine.
- La chaîne de certificats et ses attributs doivent être traités correctement par tous les composants (par exemple péremption du certificat / expired).
- Les mécanismes et les fonctions définis dans le standard du protocole de chiffrement doivent être pris en compte et supportés (par exemple la version du protocole de chiffrement, forward secrecy etc.).

2.5. Un concept de droits d'accès a-t-il été créé et mis en œuvre?

Oui → aller à la question 2.6

Non → déchiffrement non admissible

- La proportionnalité et la sécurité des données doivent être garantis grâce à des droits d'accès adéquats et spécifiques aux rôles (roled based access control) et à d'autres mesures organisationnelles pour régler effectivement les droits d'accès. Il faut établir et mettre en œuvre un concept de rôles et des droits d'accès pour l'utilisation, les accès administratifs et l'accès aux données de logs. Les principes compatibles avec la protection des données comme « need-to-know » et « least-privileges » doivent être pris en compte. Le concept doit être vérifié et actualisé régulièrement.
- L'accès par les administratrices ou administrateurs formés, y compris l'accès à un éventuel portail administratif sont à sécuriser au moyen d'une authentification à deux facteurs. Les administratrices et administrateurs doivent être explicitement rendus attentifs qu'une évaluation spécifique aux personnes ne peut être réalisée que si une base légale au sens formel et explicite existe.
- Les accès aux programmes et aux systèmes de déchiffrement tout comme les logs doivent être contrôlés régulièrement par échantillonnage par l'organe responsable. Les irrégularités doivent être documentées et évaluées.

2.6 Les logs de déchiffrement sont-ils mis en œuvre conformément à la protection des données?

Oui → lors de l'externalisation du service (serveur proxy web) aller à la question 2.7, sinon continuer avec la question 2.8

Non → déchiffrement non admissible

- Les logs d'évènements et d'utilisation générés par le déchiffrement doivent être enregistrés. Les logs doivent être conservés de manière centrale selon leur but d'utilisation (y compris les accès à l'application et aux logs de transactions), l'intégrité des logs doit être garantie.
- La durée de la conservation doit être choisie de manière proportionnée.
- Les logs doivent être contrôlés régulièrement à travers un échantillonnage par l'organe responsable. Les irrégularités doivent être documentées et évaluées.

2.7 Les exigences permettant l'externalisation du traitement des données sont-elles respectées?

- Si le déchiffrement n'est pas effectué par le fournisseur des services web lui-même mais par un tiers, les exigences permettant l'externalisation du traitement des données fixées par les lois cantonales (d'information) et de protection des données doivent être respectées.
- Les risques additionnels liés à l'utilisation d'une technologie Cloud doivent être pris en compte, évalués dans une analyse et documentés.

Oui → aller à la question 2.8

Non → déchiffrement non admissible

2.8 Toutes les exigences en lien avec le déchiffrement des connexions web sont-elles mises en œuvre?

Oui → déchiffrement des connexions web admissible

Non → déchiffrement non admissible

3 Autres informations: aide-mémoires sur le traitement des données sur mandat des autorités cantonales de protection des données

privatim	Merkblatt Cloud-spezifische Risiken und Massnahmen
Canton d'Argovie	Auslagerung von Datenbearbeitungen: Besonderheiten des Cloud Computing
Canton de Bâle-Campagne	Merkblatt Outsourcing
Canton de Bâle-Ville	Website «Handreichungen» Leitfaden Auftragsdatenbearbeitung
Canton de Genève	Fiche «Cloud computing et protection des données personelles au sein des institutions publiques genevoises»
Canton de St. Gall	Checkliste «Vereinbarungsinhalt beim Outsourcing»
Canton de Zurich	Website «Outsourcing» Leitfaden Bearbeiten im Auftrag Leitfaden Verschlüsselung der Datenablage im Rahmen der Auslagerung