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

Checkliste
Entschlüsselung von verschlüsselten Webverbindungen

1 Einleitung

Verschlüsselte Webverbindungen (https-Verbindungen) gehören zum Standard im Internet. Sie stellen eine wesentliche technische Massnahme dar zur Gewährleistung der Privatsphäre und der Informationssicherheit beim Aufrufen von Websites im Sinne der Informationssicherheitsbestimmungen in den kantonalen (Informations- und) Datenschutzgesetzen. Verschlüsselte Verbindungen schränken jedoch Schutzmassnahmen ein, wie die Filterung von Malware oder unerwünschten Inhalten. Deshalb besteht oft ein Interesse daran, dass verschlüsselte Verbindungen von Internet-Surfproxies oder ähnlichen Anwendungen entschlüsselt werden können.

Die Entschlüsselung tangiert nicht nur die Privatsphäre der betroffenen Personen, sondern auch die Integrität und Authentizität von Online-Transaktionen. Eine Risikoabwägung sowie datenschutzkonforme Massnahmen bei der Umsetzung sind zwingend.

Die Checkliste unterstützt die verantwortlichen öffentlichen Organe beim Entscheid über die Entschlüsselung und die damit beauftragten internen oder externen Stellen bei der Umsetzung der Massnahmen zur datenschutzkonformen Entschlüsselung von verschlüsselten Webverbindungen.

2 Checkliste:

«Ist eine datenschutzkonforme Entschlüsselung von verschlüsselten Webverbindungen möglich?»

2.1 Wurde eine Risikoanalyse und -beurteilung vorgenommen?

Ja → weiter zu Frage 2.2

Nein → Entschlüsselung nicht zulässig

- Es ist aufzuzeigen, dass die Massnahmen zur Risikominderung das Aufbrechen einer Verbindung rechtfertigen.

2.2 Ist die Transparenz der Entschlüsselung sichergestellt?

Ja → weiter zu Frage 2.3.

Nein → Entschlüsselung nicht zulässig.

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

- Der Zweck der Entschlüsselung sowie die dafür genügende Rechtsgrundlage sind klar zu dokumentieren.
- Es ist zu regeln, in welchen Fällen Verbindungen entschlüsselt werden.
- Die Nutzerinnen und Nutzer sind vor der Entschlüsselung der Verbindung über die damit verbundenen Risiken zu informieren.
- Auf einer den Nutzerinnen und Nutzern zugänglichen Website sind die nötigen Informationen aufzuführen zum Thema Entschlüsseln von Verbindungen. Auf der Website sind Dokumentationen über Prozesse und Abläufe zur Verfügung zu stellen.
- Die Nutzerinnen und Nutzer sind darüber zu informieren, wie sie erkennen, ob das Zertifikat von der Website stammt.
- Zertifikatsfehler und -probleme sind technisch korrekt an den Client-Browser weiterzugeben und den Nutzerinnen und Nutzern transparent zu machen (Fehlermeldung).

2.3 Besteht ein Prozess für Ausnahmen?

Ja → weiter zu Frage 2.4

Nein → Entschlüsselung nicht zulässig

- Es ist ein Prozess zu implementieren, in dem Nutzerinnen und Nutzer eine Ausnahme von der Entschlüsselung von Websites beantragen können. Vor dem Entscheid über die Genehmigung der Ausnahme ist eine Interessenabwägung vorzunehmen, und die Antragstellerin oder der Antragsteller ist über den Entscheid zu informieren.

2.4 Wird eine gültige und vertrauenswürdige Zertifikatskette verwendet?

Ja → weiter zu Frage 2.5

Nein → Entschlüsselung nicht zulässig

- Für die Entschlüsselung der Verbindungen ist ein für das verantwortliche öffentliche Organ ausgestelltes und gültiges Zertifikat zu verwenden.
- Wenn eine Website ein abgelaufenes Zertifikat (expired) benützt, sind die Nutzerinnen und Nutzer darüber zu informieren. Sie müssen die Wahlmöglichkeit bekommen, die Website aufzurufen oder nicht aufzurufen.
- Wenn eine aufgerufene Website ein Zertifikat einer nicht vertrauenswürdigen Certificate Authority (CA) benützt, sind die Nutzerinnen und Nutzer darüber zu informieren. Sie müssen die Wahlmöglichkeit bekommen, die Website aufzurufen oder nicht aufzurufen.
- Wenn eine aufgerufene Website ein zurückgezogenes Zertifikat (revoked) verwendet, ist die Verbindung zu blockieren und die Nutzerinnen und Nutzer sind darüber zu informieren.
- Die Gültigkeitsdauer des für die Entschlüsselung generierten Zertifikats ist gleich lang oder kürzer als die des Originalzertifikats.
- Die Zertifikatskette und ihre Attribute werden von allen Komponenten korrekt behandelt (zum Beispiel Zertifikat abgelaufen / expired).
- Die im Standard des Verschlüsselungsprotokolls definierten Mechanismen und Funktionen sind zu beachten und zu unterstützen (beispielsweise Version des Verschlüsselungsprotokolls, Forward Secrecy usw.).

2.5. Wurde ein Berechtigungskonzept erstellt und umgesetzt?

Ja → weiter zu Frage 2.6

Nein → Entschlüsselung nicht zulässig

- Die Verhältnismässigkeit und die Datensicherheit sind durch angemessene rollenspezifische Zugangsrechte (Role Based Access Control) und weitere organisatorische Massnahmen zur effektiven Zugriffsregelung sicherzustellen. Für die Anwendung, die administrativen Zugänge und den Zugriff auf Protokolldaten ist ein Rollen- und Berechtigungskonzept zu erstellen und umzusetzen. Datenschutzfreundliche Prinzipien wie «need-to-know» und «least-privileges» sind dabei zu berücksichtigen. Das Konzept ist regelmässig zu überprüfen und zu aktualisieren.
- Der Zugriff durch dafür geschulte Administratorinnen oder Administratoren, inklusive Zugriff auf ein mögliches Administrationsportal, sind durch eine Zwei-Faktor-Authentifizierung abzusichern. Die Administratorinnen und Administratoren sind ausdrücklich darauf hinzuweisen, dass eine personenbezogene Auswertung nur gestützt auf eine ausdrückliche Grundlage im formellen Gesetz erfolgen darf.
- Die Zugriffe auf die Anwendungen und die Systeme zur Entschlüsselung sowie die Protokolldaten sind stichprobenmässig durch das verantwortliche Organ zu überprüfen. Unregelmässigkeiten sind zu erfassen und auszuwerten.

2.6 Ist die Protokollierung der Entschlüsselung datenschutzkonform umgesetzt?

Ja → bei Auslagerung der Dienstleistung (Internet-Surfproxy) weiter zu Frage 2.7, sonst weiter zu Frage 2.8

Nein → Entschlüsselung nicht zulässig

- Die durch die Entschlüsselung entstehenden Ereignis- und Anwendungsprotokolle sind aufzuzeichnen. Die Protokolle sind gemäss ihrem Verwendungszweck zentral aufzubewahren (inklusive Zugriffe auf die Anwendung sowie auf die Protokolldaten), die Integrität der Protokolldaten ist sicherzustellen.
- Die Aufbewahrungsdauer ist verhältnismässig zu wählen.
- Die Protokolldaten sind regelmässig durch das verantwortliche Organ stichprobenmässig zu überprüfen. Unregelmässigkeiten sind zu erfassen und auszuwerten.

2.7 Sind die Anforderungen an die Auslagerung von Datenbearbeitungen eingehalten?

- Erfolgt die Entschlüsselung nicht durch den Anbieter der Webdienstleistungen selbst, sondern durch einen Dritten, sind die Anforderungen an die Auslagerung von Datenbearbeitungen nach dem kantonalen (Informations- und) Datenschutzgesetz einzuhalten.
- Zusätzliche Risiken, die durch die Nutzung einer Cloud-Lösung entstehen, müssen bewertet und in einer Beurteilung berücksichtigt und dokumentiert werden.

Ja → weiter zu Frage 2.8

Nein → Entschlüsselung nicht zulässig

2.8 Sind sämtliche Anforderungen an die Entschlüsselung von Webverbindungen umgesetzt?

Ja → Entschlüsselung von Webverbindungen zulässig

Nein → Entschlüsselung nicht zulässig

3 Weiterführende Informationen: Leitfäden Auftragsdatenbearbeitung der kantonalen Datenschutzbeauftragten

privatim	Merkblatt Cloud-spezifische Risiken und Massnahmen
Kanton Aargau	Auslagerung von Datenbearbeitungen: Besonderheiten des Cloud Computing
Kanton Basel-Landschaft	Merkblatt Outsourcing
Kanton Basel-Stadt	Website «Handreichungen» Leitfaden Auftragsdatenbearbeitung
Kanton Genf	Fiche «Cloud computing et protection des données personelles au sein des institutions publiques genevoises»
Kanton St. Gallen	Checkliste «Vereinbarungsinhalt beim Outsourcing»
Kanton Zürich	Website «Outsourcing» Leitfaden Bearbeiten im Auftrag Leitfaden Verschlüsselung der Datenablage im Rahmen der Auslagerung