dsb
datenschutzbeauftragte
des kantons zürich

Checkliste

Entschlüsselung von Webverbindungen

1 Einleitung

Die verschlüsselten Webverbindungen (https-Verbindungen) gehören zum Standard im Internet. Sie sind eine wesentliche technische Massnahme zur Gewährleistung der Privatsphäre und der Informationssicherheit beim Aufrufen von Websites im Sinne von § 7 des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4). Die verschlüsselten Verbindungen schränken jedoch die Schutzmassnahmen ein, wie die Filterung von Malware oder unerwünschten Inhalten. Deshalb kann es sinnvoll sein, dass die verschlüsselten Verbindungen von Internet-Surfproxies oder ähnlichen Anwendungen entschlüsselt werden.

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

Diese Checkliste unterstützt die öffentlichen Organe bei der Umsetzung der Massnahmen zur datenschutzkonformen Entschlüsselung der verschlüsselten Webverbindungen.

2 Checkliste

Ist eine datenschutzkonforme Entschlüsselung von Webverbindungen möglich?

1. Wurde eine Risikoanalyse und -beurteilung vorgenommen?

Ja	weiter zu 2.
Nein	Entschlüsselung nicht möglich

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

---

2. Ist die Transparenz der Entschlüsselung sichergestellt?

Ja	weiter zu 3.
Nein	Entschlüsselung nicht möglich

- Der Zweck der Entschlüsselung sowie die Rechtsgrundlage sind klar zu dokumentieren.
- Es ist zu regeln, in welchen Fällen die Verbindungen entschlüsselt werden beziehungsweise werden können.
- Die Nutzerinnen und Nutzer sind vor der Entschlüsselung der Verbindung über die damit verbundenen Risiken zu informieren.
- Die notwendigen Informationen zur Entschlüsselung von Verbindungen sind auf einer Website aufzulisten. Dort müssen die Prozesse und die Abläufe dokumentiert sein. Die Website muss den Nutzerinnen und Nutzern zugänglich sein.
- Die Nutzerinnen und Nutzer sind darüber zu informieren, wie sie erkennen, ob das Zertifikat von der jeweiligen Website stammt.
- Die Zertifikatsfehler und -probleme sind technisch korrekt an den Browser der Nutzerinnen und Nutzer weiterzureichen und ihnen transparent zu machen (Fehlermeldung).

---

3. Besteht ein Prozess für Ausnahmen?

Ja	weiter zu 4.
Nein	Entschlüsselung nicht möglich

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

---

4. Wird eine gültige und vertrauenswürdige Zertifikatskette verwendet?

Ja	weiter zu 5.
Nein	Entschlüsselung nicht möglich

- Für die Entschlüsselung der Verbindungen ist ein gültiges Zertifikat zu verwenden, das vom öffentlichen Organ ausgestellt wurde.
- Wenn eine Website ein abgelaufenes Zertifikat (expired) benützt, sind die Nutzerinnen und Nutzer darüber zu informieren.
- Wenn eine aufgerufene Website ein Zertifikat einer nicht vertrauenswürdigen Certificate Authority (CA) benützt, sind die Nutzerinnen und Nutzer darüber zu informieren.

- Wenn eine aufgerufene Website ein zurückgezogenes Zertifikat (revoked) verwendet, ist die Verbindung zu blockieren und die Nutzerinnen und Nutzer sind darüber zu informieren.
- Das für die Entschlüsselung generierte Zertifikat muss gleich lang gültig sein wie das Originalzertifikat. Es kann auch kürzer gültig sein.
- 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.).

---

5. Wurde ein Berechtigungskonzept erstellt und umgesetzt?

Ja	weiter zu 6.
Nein	Entschlüsselung nicht möglich

- 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 die Administratorinnen oder Administratorensind durch eine Zwei-Faktor-Authentifizierung abzusichern. Dies gilt auch für den Zugriff auf ein mögliches Administrationsportal.
- 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.

---

6. Ist die Protokollierung der Entschlüsselung datenschutzkonform umgesetzt?

Ja	bei der Auslagerung der Dienstleistung (Internet-Surfproxy) weiter zu 7, sonst weiter zu 8.
Nein	Entschlüsselung nicht möglich

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

7. Sind die Anforderungen an die Auslagerung der Datenbearbeitungen eingehalten?

– Erfolgt die Entschlüsselung nicht durch den Anbieter der Webdienstleistungen selbst, sondern durch einen Dritten, so sind die Anforderungen an die Auslagerung von Datenbearbeitungen gemäss § 6 IDG einzuhalten.
– Bei der Nutzung einer Cloud-Lösung müssen die zusätzlichen Risiken bewertet, in einer Beurteilung berücksichtigt und dokumentiert werden.

Ja	weiter zu 8.
Nein	Entschlüsselung nicht möglich

8. Sind sämtliche Anforderungen an die Entschlüsselung von Webverbindungen umgesetzt?

Ja	Entschlüsselung von Webverbindungen möglich
Nein	Entschlüsselung nicht möglich

3 Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich
Leitfaden Bearbeiten im Auftrag

V 1.4 / August 2023