Bestandesaufnahme

Leitfragen an die eigene Organisation

# Von interner IT/OT Abteilung auszufüllen:

|  |  |
| --- | --- |
| Name Lieferant: |  |
| Dienstleistung des Lieferanten: |  |
| Ansprechpartner innerhalb der eigenen Organisation: |  |
| Kontakt: |  |
| Fragebogen Nr.: |  |

# Dienstleistungen des Lieferanten

| 1.1 | Sind die Dienstleistungen des Lieferanten oder Partner für unsere Geschäftsprozesse wichtig? | Ja  Nein  Ich weiss es nicht |
| --- | --- | --- |
|  | Dienstleistungen beschreiben. |  |

# IT/OT Produkte des Lieferanten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.1 | Beliefert uns der Lieferant mit IT- oder OT-Produkten die in unseren (kritischen) Umgebungen ausgeführt werden? | | Ja ☐  Nein ☐  Ich weiss es nicht ☐ | |
|  | | IT/OT-Produkte beschreiben. |  |

# Zugriffe des Lieferanten auf interne Systeme

| 3.1 | Hat der Lieferant Zugriff auf (kritische) Systeme, die von uns betrieben werden? | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
| --- | --- | --- |
|  | Wenn mit Ja beantwortet, bitte um Benennung der Art von Daten, die in diesen Systemen gespeichert werden. |  |
|  | Interne Daten unserer Organisation | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Interne Geschäftsdaten inkl. Daten von Kunden, Partner unserer Organisation | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Mitarbeiterdaten unserer Organisation | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Personendaten von Kunden / Partnern unserer Organisation | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Mitarbeiterkenndaten (Passwörter) unserer Organisation | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Weitere. |  |
| 3.2 | Falls in der eigenen Organisation zutreffend: Sind beim Lieferanten die Mitarbeitenden, welche Zugriff auf Computer-Systeme haben, die innerhalb der IT-Netzwerke unserer Organisation betrieben werden oder für Computer-Systeme, welche Daten unserer Organisation bearbeiten, vor Zugriffserteilung auf ebendiese Computer Systeme, persönliche Background-Checks durchgeführt worden? | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Wenn mit Nein beantwortet, bitte Vertragsbestandteil «Rechtevergabe» entsprechend anpassen. |  |

# Systeme, die durch den Lieferanten betrieben werden

| 4.1 | Betreibt der Lieferant Systeme für uns, die wir für kritische Geschäftsprozesse benötigen? Dies sind z. B. SaaS basierte Anwendungen für Rekrutierung, Payroll oder Kollaborationssysteme. | | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
| --- | --- | --- | --- |
| 4.2 | | Welche Daten werden dabei erhoben resp. gespeichert? |  |
|  | | Personendaten (Name, Vorname, Geburtsdatum, Geburtsort, AHV - Nr., Pass- resp. ID-Nummer, Anschrift, Telefonnummer, E-Mail-Adresse, Standort- IP Adressen usw.) | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | | Besonders schützenswerte Personendaten[[1]](#footnote-1) (Angaben zur Gesundheit, Religion, politischer und weltanschaulicher Meinung, sexueller Orientierung und Intimsphäre, biometrische und genetische Daten, Strafverfolgungseinträge usw., gemäss gültigem CH-Datenschutzgesetz.) | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | | Kreditkartendaten | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | | Verbindungsdaten (IP-Adresse, Geolocation, GPS-Positionsdaten, sonstige Telemetriedaten, usw.) | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |

# Cyberangriff auf den Lieferanten

Diese Fragen sind relevant, sofern die Dienstleistungen des Lieferanten für den Geschäftsprozess relevant sind, respektive wenn Daten der Organisation bearbeitet werden.

| 5.1 | Ist in unserer Organisation sichergestellt, dass bei einem schwerwiegenden Cyberangriff auf den Lieferanten nicht mit Datenverlust unsererseits gerechnet werden muss? | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
| --- | --- | --- |
|  | Wenn mit Nein beantwortet, bitte um Beschreibung der angedachten Massnahmen (bspw. Isolation / Überwachung von Zugriffen / MFA). |  |

| 5.2 | Sind wir in der Lage, unsere Geschäftsprozesse weiterhin zu betreiben, wenn der Lieferant (für längere Zeit) ausfällt? | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
| --- | --- | --- |
|  | Wenn mit Nein beantwortet, bitte um Beschreibung der angedachten Massnahmen (bspw. Umgang mit einem Ausfall / Notfallplan / Offline Backups): |  |
| 5.3 | Sind wir in der Lage, unsere Dienstleistungen weiterhin anzubieten, wenn der Lieferant (für längere Zeit) ausfällt? | Ja ☐  Nein ☐  Ich weiss es nicht ☐ |
|  | Wenn mit Nein beantwortet, bitte um Beschreibung der angedachten Massnahmen (bspw. Umgang mit einem Ausfall / Notfallplan): |  |

1. Unter die Bezeichnung «besonders schützenswerte Daten» fallen all jene Daten, welche bei einer Veröffentlichung, zu einem hohen Risiko für betroffene natürliche Personen führen können. [↑](#footnote-ref-1)