Bestandesaufnahme

Leitfragen an die Lieferanten

# Von interner IT/OT Abteilung auszufüllen:

|  |  |
| --- | --- |
| Lieferantennummer: |       |
| Hauptansprechpartner: |       |
| Filiale: |       |
| Tätig in den Filialen: |       |
| Fragebogen Nr.: |       |

# Von Partner auszufüllen:

|  |  |
| --- | --- |
| Name Lieferant: |       |
| Dienstleistung des Lieferanten: |       |
| Jobbezeichnung: |       |
| Datum: |       |
| Unterschrift: |       |

# Organisation im Bereich der IT-Sicherheit

| 1.1 | Ist Ihre Unternehmung im Bereich der IT-Sicherheit mit einem gültigen, anerkannten Zertifikat eines branchenspezifischen Frameworks ausgestattet (zum Beispiel ISO27001 / CoBit / BSI usw.)? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| --- | --- | --- |
|  | Wenn mit Ja beantwortet, bitte um Beschreibung:  |       |
| 1.2 | Wie ist die IT-Sicherheit in Ihrem Unternehmen geregelt. Beschreiben Sie die Funktionen von Mitarbeitenden im Bereich IT-Sicherheit und geben Sie zudem die für diesen Bereich zuständige Person (CISO, IT Security Officer, CTO usw.) an: |       |
| 1.3 | Haben Sie ein Schwachstellenmanagement? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 1.4 | Über welchen Kanal und wie rasch informiert Ihr Unternehmen unsere Organisation beim Entdecken einer Schwachstelle? |       |
| 1.5 | Über welchen Kanal und wie rasch informiert Ihr Unternehmen unsere Organisation bei einem internen IT-Sicherheitsvorfall? |       |

# Organisation im Bereich der Datensicherheit

| 2.1 | Hält Ihr Unternehmen bei der Bearbeitung von Daten die Anforderungen und Vorgaben des Datenschutzgesetzes (DSG) ein? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| --- | --- | --- |
|  | Wenn mit Nein beantwortet, bitte um Begründung:  |       |
| 2.2 | Hat Ihr Unternehmen ein aktuelles Diagramm, aus welchem hervorgeht, wie sensible Daten in seine Systeme gelangen und wo sie schliesslich gespeichert werden? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
|  | Wenn mit Nein beantwortet: Wäre Ihr Unternehmen bereit, ein solches Diagramm zu erstellen? | Ja ☐Nein ☐Ich weiss es nicht ☐ |

| 2.3 | Nutzt Ihr Unternehmen moderne, gewartete und dem Industriestandard entsprechende Verschlüsselungs-Methoden, um sensible Daten bei der Übertragung zwischen Systemen und im Ruhestand in Online-Datenspeichern und Backups zu schützen? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| --- | --- | --- |
| 2.4 | Hat Ihr Unternehmen ein Konzept betreffend Datenvernichtung (Daten definitiv löschen)? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 2.5 | 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. |       |

# Computer Systeme

| 3.1 | Setzt Ihre Unternehmung eigens betriebene Systeme für die für uns erbrachten Dienstleistungen ein?  | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| --- | --- | --- |
|  | Wenn Nein, falls Systeme durch Drittanbieter gestellt werden; welcher Anbieter ist dies? |       |
| 3.2 | Sind die Systeme mit einer aktualisierten EDR/XDR Lösung ausgestattet und werden Vorfälle, welche durch diese «erweiterten Antivirus Lösungen» entdeckt werden, bei Ihrem Unternehmen aktiv gemanagt oder durch ein ausgelagertes SOC geprüft? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 3.3 | Wie rasch können diese Systeme nach einem Service-Unterbruch resp. Cybervorfall wieder in den Normalbetrieb geführt werden? |       |

# Zugriffe auf Computer Systeme, andere Geräte, Workloads

| 4.1 | Werden für die Zugriffe auf die oben beschriebenen Systeme nur personalisierte Benutzerkonten genutzt? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| --- | --- | --- |
| 4.2 | Nutzen Ihre Mitarbeitenden für die Erledigung der regulären Tagesarbeit andere Benutzerkonten als jene, welche für den Zugriff auf die von unserer Organisation zur Verfügung gestellten Systeme oder solche, die Daten von unserer Organisation enthalten, berechtigt sind?  | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 4.3 | Setzen Sie den Least-Privilege-Ansatz bei Ihren Mitarbeitenden um?  | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 4.4 | Ist sichergestellt, dass Benutzerkonten mit erhöhten Privilegien nicht permanent über dieses Berechtigungsniveau verfügen? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 4.5 | Falls zur Ausübung der Dienstleistung sogenannte «Service-Accounts» eingesetzt werden; ist sichergestellt, dass die Credentials sicher aufbewahrt und nicht für unbefugte Mitarbeitende zugänglich sind? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 4.6 | Werden Zugriffe auf Systeme, welche Daten unserer Organisation beinhalten/bearbeiten mittels MFA geschützt, falls diese von externen Zonen angesprochen werden (via VPN oder Inter-Webseitenzugriff oder ähnliches)? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 4.7 | Werden sämtliche Zugriffe auf diese Systeme protokolliert, gesichert und können diese auf Wunsch durch IT-Sicherheitspersonal unserer Organisation eingesehen werden? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| 4.8 | Existiert eine schriftlich verfasste, detaillierte Passwortrichtlinie? | Ja ☐Nein ☐Ich weiss es nicht ☐ |

# Awareness

| 5.1 | Sind die Mitarbeitenden im Bereich IT-Sicherheit (mindestens zur Bedrohung mittels «Phishing») sensibilisiert und nachweislich geschult worden? | Ja ☐Nein ☐Ich weiss es nicht ☐ |
| --- | --- | --- |
| 5.2 | Ist ein solches Schulungsprogramm durch das IT-Sicherheitspersonal unserer Organisation einsehbar? | Ja ☐Nein ☐Ich weiss es nicht ☐ |