SHS - STAHL-HOLDING-SAAR

Richtlinie zum Zugriff auf IT-Systeme der SHS-Gruppe für Fremdfirmen

Zwischen dem Auftraggeber und der Firma besteht ein Vertragsverhältnis betreffend Inbetriebnahme, Gewährleistung oder Wartung von Hard- und Software, bzw. weiterer Leistungen, die Zugriff auf und/oder Nutzung von unserer internen IT-Struktur (oder damit verbundener Systemen und Informationen) erfordern.

Anforderungen an die Mitarbeiter der Firma

Alle Mitarbeiter der Firma, die Zugriff auf interne Systeme erhalten, sind dafür entsprechend ausgebildet und sensibilisiert. Dies gilt insbesondere für folgende Punkte:

- Die Mitarbeiter sind mit den grundlegenden Aspekten der Informationssicherheit hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen vertraut und wissen wie diese Ziele in ihrer täglichen Arbeit zu gewährleisten sind.

- Die Mitarbeiter sind verpflichtet Verschwiegenheit über die, ihnen zur Kenntnis gelangenden, betriebsbezogenen und personenbezogenen Daten zu wahren, diese weder unbefugt zu kopieren oder zu sammeln noch zu nutzen oder zu verarbeiten. Die Pflicht besteht auch nach Vertragserfüllung zeitlich unbegrenzt fort. Diese Verpflichtung gilt auch gegenüber dem Arbeitgeber.

- Die Firma überwacht die Einhaltung dieser Richtlinie durch ihre Beschäftigten und wird den hier vereinbarten Datenschutz und die Datensicherheit durch geeignete technische und organisatorische Maßnahmen sicherstellen.

- Zugänge auf interne Systeme erfolgen personalisiert. Für jeden Mitarbeiter der Firma, der Zugriff benötigt, ist ein separater, personalisierter Antrag auf Zugang zu stellen.

- Der Auftraggeber hat das Recht, Mitarbeiter der Firma nach Sicherheitsverletzungen abzulehnen.

Anforderungen an IT Systeme der Firma (von denen aus der Zugriff erfolgt)

Der Auftraggeber verlangt generell, dass IT Systeme mit denen auf das interne Netzwerk oder interne Systeme zugegriffen wird über einen aktuellen Sicherheitsstandard verfügen. Alle SHS-Systeme werden gemäß dieser Vorgabe bereitgestellt, betrieben und gewartet. Der Auftraggeber bietet daher der Firma an, für ihre Tätigkeiten SHS-eigene Systeme zu nutzen, die diesem Standard entsprechen. Dadurch können die Risiken durch Verwendung nicht konformer IT-Systeme drastisch reduziert werden. Dies betrifft sowohl mögliche Cyber Attacken, als auch Verzögerungen im Projekt auf Grund von Nichtkonformitäten. Zudem übernimmt der Auftraggeber bei bestimmungsgemäßem Gebrauch die Verantwortung für seine Systeme.

Gibt es zwingende Gründe, dass Zugriffe nur von IT Systemen der Firma selbst erfolgen können und eine Nutzung von durch den Auftraggeber bereitgestellten Systemen nicht möglich ist, muss die Firma die Verantwortung für den geforderten Sicherheitsstandard selbst übernehmen:

- Die Firma verpflichtet sich, dass IT-Systeme, mit denen auf das Netzwerk oder IT-Systeme des Auftraggebers zugegriffen werden, entsprechend der Kritikalität der betroffenen Informationswerte geschützt sind. Insbesondere ist gewährleistet, dass die getroffenen Maßnahmen den „Stand der Technik“ berücksichtigen, beispielsweise durch geeignete Vorgehensweisen gemäß der ISO/IEC

27001 bzw. BSI Grundschutz. Die Minimalanforderungen „Basismaßnahmen der Cybersicherheit“ (BSI CS-006 Version 2.0) werden eingehalten. Von besonderer Bedeutung sind daraus die Absätze 3.3, 3.4, 4, 6, 7, 8.

Weitere Rechte und Pflichten

- Die Firma und der Mitarbeiter stimmen der Protokollierung der durchgeführten Tätigkeiten und eventueller Verarbeitung personenbezogener Daten in Verbindung mit den vertraglich vereinbarten Tätigkeiten zu.

- Der Verlust eines für den Zugang eingerichteten Endgerätes muss dem Auftraggeber angezeigt werden.

- Die Firma verpflichtet sich, den Zugang nicht zu benutzen, wenn sich Sicherheitsvorfälle ereignet haben, die auf das Auftraggeber-interne Netzwerk auswirken oder übergreifen könnten. Der Auftraggeber ist über solche Vorgänge zeitnah zu informieren.

- Der Auftraggeber ist berechtigt, das mitgebrachte IT-System der Firma zu auditieren (technisch durch Viren- und Schwachstellenscanner). Bei Verdachtsfällen (bspw. potentielle Verbreitung von Schadcode) darf der Auftraggeber das Gerät zur forensischen Analyse einbehalten.

- Fernzugriff bei einem Client-to-Site-VPN erfolgt immer über eine Zweifaktor-Authentifizierung (zum Beispiel OTP).

- Die Einschaltung bzw. Beauftragung von Subunternehmern ist ausgeschlossen, oder muss explizit vertraglich geregelt sein. Für Subunternehmer und ihre Mitarbeiter gelten die gleichen Anforderungen. Eine Delegation der Verantwortung/Haftung auf Subunternehmer ist ausgeschlossen.

- Vor der Einrichtung des Zugriffes müssen alle lizenzrechtlichen Fragen geklärt sein. Der Zugriff darf nicht zu lizenzseitigen Belastungen des Auftraggebers führen.

- Der Auftraggeber kann jederzeit ohne Einhaltung einer Frist bereits gewährte Zugänge der Firma oder deren Mitarbeiter sperren oder entziehen, wenn einer der nachstehenden Punkte vorliegt:

    - Verdacht auf schädliches Verhalten des IT-Systems, zum Beispiel bei Alarmierung durch interne Überwachungssysteme, oder sonstigen Indizien, die auf ein nicht konformes Verhalten hindeuten (vgl. Anforderungen an die IT Systeme der Firma).

    - Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung (DSGVO)

    - Nichteinhaltung dieser Richtlinie

    - Nichteinhaltung ergänzender spezifischer Abreden im Zusammenhang mit der Zugangsregelung oder der Informationssicherheit

    - Verstoß gegen die Verschwiegenheitspflicht

    - Weigerung der Firma ein Audit oder Stichprobenaudit durchführen zu lassen