Anforderungen an die Informationssicherheit für Auftragnehmer der EnBW AG ›

EnBW-HST-026

Dokumentinformationen

Geltungsbereich	EnBW-Konzern
Version	1.0
Klassifizierungsstufe	Öffentlich
Zusammenfassung	Dieses Dokument beschreibt verbindliche Anforderungen an die Informationssicherheit bei Auftragnehmern der EnBW AG
Inkrafttreten	05.04.2023
Letzte Aktualisierung	05.04.2023
Fachlich zuständige Stelle	CISO (C-TS)
Freigegeben durch	Markus Penn, Konzern-ISM, C-TSM
Freigegeben am	05.04.2023
Anlagen	-

Anforderungen an die Informationssicherheit für Auftragnehmer der EnBW AG >
EnBW-HST-026

Änderungshistorie

Version	Aktualisierungs-datum	FZS/Autor	Kurzbeschreibung
1.0	05.04.2023	CISO	Initiale Version

Inhalt

1 Anwendungsbereich

Diese Anforderungen an die Informationssicherheit sind Grundlage für jeden Lieferanten/Auftragnehmer (nachfolgend „Auftragnehmer“) der EnBW Energie Baden-Württemberg AG (nachfolgend „EnBW“), die im Rahmen der Abwicklung eines Vertragsverhältnisses Zutritt zu Gebäuden oder Räumlichkeiten bzw. Zugang und/oder Zugriff auf elektronische Informationen bzw. Informationssysteme der EnBW erhalten. Die Auftragnehmer sind verpflichtet, die Regelungen dieser Anlage zwingend einzuhalten, sofern keine abweichenden Regelungen vertraglich vereinbart wurden.

Diese Anlage verpflichtet alle Auftragnehmer, unabhängig davon, ob ein IT-Arbeitsplatz-System der EnBW zur Verfügung gestellt wird oder mit eigenen Systemen oder mit Anschluss zu Ressourcen im EnBW-Kommunikationsnetzwerk auf die EnBW-Informationssysteme zugegriffen wird.

2 Informationssicherheitsanforderungen an Auftragnehmer

Jeder Auftragnehmer stellt auf Anfrage einen Ansprechpartner für Informationssicherheit zur Verfügung und hat die folgenden Grundsätze zu beachten:

2.1 Allgemeine Verpflichtungen

Dem Auftragnehmer ist bewusst, dass die EnBW den Leistungsgegenstand als Betreiber kritischer Infrastrukturen zur Energieversorgung einsetzt und daher erhöhten gesetzlichen und regulatorischen Anforderungen im Bereich der Informationssicherheit unterliegt, insbesondere nach dem BSIG und dem EnWG.

Der Auftragnehmer muss ein formelles Informationssicherheitsmanagement-System (ISMS) etabliert haben und dieses regelmäßig weiterentwickeln und aktualisieren.

Der Auftragnehmer hat die Lieferungen und Leistungen so zu erbringen, dass sie zum Zeitpunkt der Leistungserbringung den aktuellen gesetzlichen und regulatorischen Anforderungen im Hinblick auf die Informationssicherheit der EnBW und insbesondere zum Schutz der IT-Infrastruktur der EnBW genügen. Er ist verpflichtet, angemessene Vorkehrungen zu treffen, um sicherzustellen, dass die von ihm verarbeiteten Daten dem Stand der Technik im Hinblick auf die Informationssicherheit entsprechend vor Angriffen oder sonstigen Vorkommnissen mit nachteiligen Auswirkungen auf Anlagen, Systeme, Maschinen, Computer, Netzwerke oder andere Infrastruktur und Ressourcen durch unautorisierten Zugang, Zerstörung, Beschädigung, Veröffentlichung oder Veränderung von Informationen, "*denial of service attacks*" oder anderen Angriffen geschützt sind.

Der Auftragnehmer stellt der EnBW die IT-sicherheitsrelevanten Protokolldaten zur Verfügung, die im Zusammenhang mit der Verarbeitung von EnBW-Informationen anfallen. Dies muss, soweit möglich, automatisiert und in Echtzeit erfolgen, etwa durch Schaffung eines entsprechenden Zugangs, aber in jedem Falle unverzüglich.

Der Auftragnehmer ergreift für eigene datenverarbeitende Systeme, auf denen Informationen der EnBW verarbeitet werden, ausreichende Erkennungs- und Vorbeugungsmaßnahmen vor Schadsoftware und implementiert geeignete Wiederherstellungsmaßnahmen.

Besondere Sicherungseinstellungen, -systeme oder sonstige Vorkehrungen auf datenverarbeitenden Systemen der EnBW (z. B. zum Schutz vor Schadsoftware, Verschlüsselungen) dürfen vom Auftragnehmer, sofern nicht explizit abweichend vereinbart, nicht außer Betrieb genommen, umgangen oder in sonstiger Weise verändert werden.

Der Auftragnehmer holt regelmäßig und zeitnah Informationen über technische Schwachstellen in von ihm verwendeten Systemen ein und ergreift angemessene Maßnahmen.

Der Auftragnehmer erfüllt die Vorgaben der EnBW zur sicheren Übertragung von vertraulichen Informationen und Daten:

- Verschlüsselung der Daten bei elektronischer Übertragung über unsichere Netze
- Versand von Papierdokumenten in verschlossenen Umschlägen
- Sicherstellen, dass nur berechtigte Empfänger die Informationen erhalten.

Soweit die EnBW dem Auftragnehmer streng vertrauliche Informationen übermittelt, schließen die Parteien eine gesonderte Vereinbarung über deren Verwendung. Streng vertrauliche Informationen bezeichnen solche Informationen, die von der EnBW als „streng vertraulich“ eingestuft werden.

Der Auftragnehmer hat sicherzustellen, dass die Einhaltung dieser Informationssicherheitsanforderungen Vertragsbestandteil der Mitarbeiter des Auftragnehmers ist.

2.2 Informationspflichten des Auftragnehmers

Änderungen der Lieferkette, Eigentümerwechsel sowie etwaige geänderte Grundvoraussetzungen der Geschäftsbeziehung, insbesondere die Aberkennung oder der Ablauf bestehender Zertifizierungen, sind unverzüglich der EnBW zu melden.

Der Auftragnehmer etabliert einen Vorfallmanagementprozess, um effektiv auf Ereignisse, Störungen und Vorfälle reagieren zu können, die die Dienstleistung betreffen könnten. Hierbei müssen Meldewege und die Kommunikation zwischen Auftragnehmer und EnBW festgelegt werden.

Der Auftragnehmer informiert die EnBW unverzüglich über Schwachstellen, Ereignisse, Störungen und Vorfälle, die einen Einfluss auf die Sicherheit von Informationen und die Qualität des Liefergegenstandes haben könnten und stimmt deren Handhabung mit der EnBW ab.

2.3 Verfügbarkeit von Daten

Hinsichtlich der Verfügbarkeit von Daten und Betriebsleistungen ist der Auftragnehmer in Abstimmung mit EnBW verpflichtet:

- alle von ihm verarbeiteten Daten regelmäßig zu sichern und diese Sicherungen an einem sicheren Ort aufzubewahren,
- über einen Notfallplan zu verfügen, der beschreibt, wie im Falle von Sicherheitsvorfälle oder anderen Notfällen vorgegangen wird und
- angemessene Maßnahmen zur Gewährleistung des Schutzes von Daten im Falle von Notfällen, wie zum Beispiel Stromausfällen oder Naturereignissen, vorzuhalten.

2.4 Zugang und Zugriff des Auftragnehmers auf EnBW-Systeme

Der Auftragnehmer ist verpflichtet, über ein Verfahren zur regelmäßigen Überprüfung von Zugriffsrechten zu verfügen, um sicherzustellen, dass ausschließlich autorisierte Personen auf datenverarbeitende Systeme der EnBW zugreifen können.

Die Mitnahme von Arbeitsergebnissen oder IT-Systemen der EnBW aus den Geschäftsräumen der EnBW ist nur im Rahmen der vertraglich vereinbarten Leistungserbringung zulässig und bedarf der vorherigen schriftlichen Genehmigung der EnBW.

Die hinterlegten Authentifizierungsinformationen (Kennungen und Passwörter) auf datenverarbeitenden Systemen der EnBW müssen personenscharf verwandt werden. Eine Weitergabe oder Offenlegung für Dritte ist untersagt.

Der Auftragnehmer stellt sicher, dass nur die Mitarbeiter Zugang zu Informationen der EnBW erhalten, die auch an der Lieferleistung mitwirken.

Der Zugang und Zugriff auf die datenverarbeitenden Systeme der EnBW darf nur über die jeweils von der EnBW zur Verfügung gestellten Endgeräte, Schnittstellen, Dienste und für die vereinbarten Zwecke und Aufgaben erfolgen.

Der Auftragnehmer setzt für die eigenen Systeme, auf denen Informationen der EnBW verarbeitet werden, ein nach Stand der Technik sicheres Anmeldeverfahren (z. B. Multi-Faktor-Authentifizierung oder

Nutzung starker Kennwörter) für den Zugang zu diesen Systemen und Anwendungen ein. Starke Kennwörter bestehen aus mindestens vierzehn (14) Zeichen, mindestens drei (3) Zeichenarten aus Zahl, Kleinbuchstabe, Großbuchstabe und Sonderzeichen; aufeinanderfolgende Zeichen wiederholen sich höchstens zweimal.

Wenn ein Fernzugang zu datenverarbeitenden Systemen der EnBW gewährt wird, dürfen nur die von EnBW vorgegebenen Gateways, Sprungserver und Dienste verwendet werden. Eine Netzkopplung oder parallele Fernzugriffe sind untersagt.

2.5 Schulung und Sicherheitsbewusstsein von Mitarbeitern des Auftragnehmers

Der Auftragnehmer muss sicherstellen, dass alle Mitarbeiter, die Zugang zu EnBW-Informationen haben, über das angemessene Sicherheitsbewusstsein und die notwendigen Kenntnisse und Fähigkeiten verfügen, um diese Daten sicher zu verarbeiten.

Der Auftragnehmer unterweist seine Mitarbeiter, die in die Lieferleistung eingebracht werden, hinsichtlich

- der Informationssicherheitsanforderungen der Lieferleistung,
- des Umgangs mit klassifizierten EnBW-Informationen und
- der Erkennung, Meldung und Handhabung von Sicherheitsvorfällen.

2.6 Kontrollrechte und -pflichten

Der Auftragnehmer muss ein Verfahren zur Überwachung und Dokumentation von Zugriffen auf EnBW-Informationen haben und regelmäßig überprüfen, ob alle Zugriffe autorisiert waren.

Die EnBW ist berechtigt, eine regelmäßige Überprüfung der Einhaltung der Informationssicherheitsvorgaben im erforderlichen Umfang durchzuführen. Die Prüfung findet in Absprache mit dem Auftragnehmer statt und wird mit einer angemessenen Vorankündigungsfrist angemeldet. Das Audit-Recht schließt das Recht ein, jede Einrichtung, die Informationen der EnBW verarbeitet, zu besichtigen und gilt ebenfalls für Unterauftragnehmer. Der Auftragnehmer stellt vertraglich sicher, dass die EnBW ihr Audit-Recht auch bei Unterauftragnehmern wahrnehmen kann. Aufwände hierfür sind nicht gesondert zu vergüten, sofern keine anderweitige vertragliche Vereinbarung getroffen wurde.

2.7 Rückgabe bei Beendigung des Vertragsverhältnisses

Der Auftragnehmer hat bei Beendigung der Beauftragung von der EnBW erhaltene Werte, z.B. Zutritts-/Zugangskarten und -token und Endgeräte sind unverzüglich zurückzugeben.