Leistungsbeschreibung

Für den EnBW Full Kritis Service Quick-Check

Karlsruhe, Apr. 2018
EnBW AG

EnBW
Energie
braucht Impulse

1 Die Herausforderung

Mit der Digitalisierung der Produktions- und Steuerungssysteme hält die IT massiv Einzug in die Industrie. Nachteil der zunehmenden Vernetzung ist, dass jede Schwachstelle im System gezielt angegriffen werden kann. Das Risiko steigt kontinuierlich, und die Manipulationen führen zu Schäden, die für Unternehmen schwerwiegend bis existenzbedrohend sein können. Die Angriffe nehmen nicht nur in Anzahl, sondern auch in ihrer Intensität zu. So infizierte das WannaCry-Virus im Mai 2017 über 200.000 Systeme in 150 Ländern.

IT-Security. Die Bundesregierung hat mit dem seit Juli 2015 gültigen IT-Sicherheitsgesetz auf die zunehmende Bedrohung durch Cyber-Angriffe im Zuge von Digitalisierung und Vernetzung reagiert.

Mit uns als Partner erreichen Sie Ihre Compliance-Ziele. Ist Ihr Unternehmen von den im IT-Sicherheitsgesetz beschlossenen Regelungen betroffen? Dann müssen Sie die Anforderungen gemäß folgender Fristen umsetzen: Bis 3. Mai 2018 in den Sektoren Energie, Informationstechnik, Telekommunikation, Ernährung, Wasser und bis 30. Juni 2019 in den Sektoren Finanz- und Versicherungswesen, Transport und Verkehr, Gesundheit.

Nutzen Sie die Erfahrung der EnBW AG. Als Betreiber von Energieerzeugungsanlagen und Netzen hat die EnBW schnell auf die Herausforderungen reagiert. Unsere Kernkraftwerke unterstehen den höchsten Sicherheitsauflagen, und wir haben als erster Kernkraftwerks-Betreiber Deutschlands die Richtlinie zur IT-Sicherheit erfolgreich umgesetzt. Die EnBW genießt Vertrauen durch die langjährige Zusammenarbeit mit den wesentlichen Behörden von Bund und Ländern und den wesentlichen Gutachtern wie TÜV und Gesellschaft für Anlagen- und Reaktorsicherheit (GRS).

Ihre IT. Sicherer. Machen. Wir wollen Ihr Unternehmen sicherer machen. In den Geschäftsfeldern Energie und Wasser und Gesundheit ist die EnBW selbst schon seit Jahren aktiv, daher konzentrieren wir uns vor allem auf diese Branchen.

Sie können einzelne Leistungen oder alle Services von uns aus einer Hand wählen. Unser Ansatz ist ganzheitlich und hat das Zusammenwirken von Mensch, Technik und Organisation im Blick: IT-Security-Beratung, Audits und Zertifizierung, IT-Betrieb.

1. EnBW Quick-Check. Analyse und Handlungsempfehlungen
2. Einführung eines Informationssicherheitsmanagementsystems (ISMS) mit Planung und Herstellung Ihrer Zertifizierungsreife bis zum Abschluss der formalen Umsetzung und „Testphase“ im Live-Betrieb.
3. Maßnahmenumsetzung entsprechend Risikobehandlungsplan.
4. Übergang in den Betrieb

Der EnBW Quick-Check für Kritische Infrastrukturen gibt Ihnen schnell einen Überblick über den aktuellen IT-Sicherheitsstatus, über Schwachstellen und Handlungsbedarf in Ihrem Unternehmen: Innerhalb von 48 Stunden nach Abschluss der Analyse erhalten Sie einen abschließenden elektronischen Bericht. Der erste Baustein auf dem Weg zur vollständigen IT-Security-Compliance Ihres Unternehmens.

2 Inhaltsverzeichnis

3 Produktbeschreibung

Im Produktangebot Full Kritis Service (FKS) hat die EnBW eine Prüfungssystematik entwickelt, die Sie schnell und zuverlässig Schwachstellen und Handlungsbedarf erkennen lässt. Der Quick-Check ist vor allem für Unternehmen geeignet, die in den Branchen Wasserwirtschaft, Energiewirtschaft und Gesundheitswesen aktiv sind, wurde aber bereits auch in anderen Branchen erfolgreich angewendet.

Sie erhalten durch den FKS Quick-Check einen schnellen, ersten Überblick über den aktuellen Reifegrad zu IT-Sicherheit (Fokus Organisation und Technik) und Datenschutz in Form von Compliance-Kennzahlen, die auf Basis der jeweils beinhalteten Normen und Vorschriften errechnet werden.

3.1 Umfang

Es werden die relevanten Anforderungen aus der ISO 27001, der aktuellen Datenschutzverordnung und der IT-Security für Ihr Unternehmen berücksichtigt und bei Ihnen vor Ort in einem Interview hinterfragt.

Dabei wird mit unserer Methode betrachtet:

- der Bereich Organisation auf Basis DIN EN ISO/IEC 27001
- der Bereich Technik auf Basis DIN EN ISO/IEC 27001 und anerkannter Regeln zur Cyber-Security
- der Bereich Datenschutz auf Basis EU-DSGVO

Die Fragestellungen aus diesen drei Verordnungen sind teilweise überlappend, daher ist eine Gesamtbewertung aus unserer Erfahrung am sinnvollsten.

Die Module können jeweils einzeln beauftragt werden. Jedes Modul enthält 8 bis 15 spezifische Fragen, die in einem gewichteten Schema zu beantworten sind. Über das jeweilige Modul erfolgt schließlich eine statistische Auswertung mit einer Compliance-Kennzahl als Ergebnis. Diese gibt bereits eine erste Einschätzung, wie konform Ihr Unternehmen hinsichtlich des normativen bzw. gesetzlichen Regelwerkes ist und in welchen Bereichen Handlungsbedarf zu erkennen ist.

Sollten während des Interviews Fragen offen bleiben, werden diese im Nachgang geklärt. Sind alle Fragen vollumfänglich beantwortet, erhalten Sie als Ergebnis innerhalb von zwei Werktagen (Montag bis Freitag) einen Bericht.

Gerne beraten wir Sie über die weitere Vorgehensweise.

3.2 Unsere Leistungserbringung

Der Quick-Check ist ein von der EnBW FKS entwickelter Fragenkatalog auf einem mobilen, speziell gehärteten und gesicherten Endgerät (Vollverschlüsselung, Zwei-Faktor-Authentifizierung, etc.).

Nach Ihrer Beauftragung wird ein Termin bei Ihnen vor Ort vereinbart. In dem halbtägigen Termin werden gemeinsam mit Ihrer Geschäftsführung bzw. einem Vertreter und den von der Geschäftsführung benannten weiteren Ansprechpartnern (z.B. Datenschutzbeauftragter, Sicherheitsbeauftragter, QS-Beauftragter, IT- und/oder Instandhaltungsleiter, etc.) die jeweils fachlich betreffenden Fragen durchgearbeitet. Die Antworten werden online nach fünf Bewertungseinheiten eingeben.

Nach Sichtung von Dokumenten und einer Qualitätsprüfung werden Ihnen dann innerhalb von zwei Werktagen nach dem Interview die Ergebnisse in einem weiteren gemeinsamen Termin erläutert.

4 Qualitätsmerkmale der Auswertung

4.1 Kontrollzielbewertung

Ihnen werden pro Kontrollziel fünf mögliche Antworten angeboten. Diese werden mit 0%, 25%, 50%, 75% und 100% bewertet. Falls ein Kontrollziel nicht relevant ist, so wird auch dies im Quick-Check erfasst, die betreffende Frage geht dann nicht in die Auswertung mit ein.

4.2 Reifegrad

Der mittels des Quick-Checks errechnete Reifegrad (Prozentwert) gibt eine erste Einschätzung hinsichtlich der Normerfüllung und zeigt bereits erkannte Abweichungen auf.

5 Mitwirkungspflicht

5.1 Kommunikation

Durch eine offene Kommunikation FKS gegenüber trägt der Auftraggeber zu einer aussagekräftigen Beurteilung hinsichtlich des Compliance-Grades bei. Alle für die Leistungserfüllung relevanten Informationen müssen zeitnah, vollständig und korrekt zur Verfügung gestellt werden.

5.2 Ressourcen

Der Auftraggeber sorgt für die Bereitstellung der notwendigen fachlich kompetenten Mitarbeiterressourcen und notwendigen Dokumentationen. Entsteht aufgrund von Nichtverfügbarkeiten relevanter Knowhow-Träger auf Seiten des Auftraggebers und/oder zusätzlich notwendiger Termine weiterer Aufwand, werden diese gemäß Punkt 8 zusätzlich in Rechnung gestellt.

5.3 Durchführungsort

Das Interview findet in den Räumlichkeiten des Auftraggebers statt.

6 Rahmenbedingungen

6.1 Haftung

Die Ergebnisse des Quick-Checks stellen eine unverbindliche Einschätzung der Zertifizierungsreife nach DIN EN ISO/IEC 27001 und Rechtskonformität mit dem IT-Sicherheitsgesetz dar. Wir übernehmen daher für die Richtigkeit der Ergebnisse und für das tatsächliche Erreichen der Zertifizierung, ggf. nach Durchführung empfohlener weiterer Maßnahmen, keine Gewähr. Dies gilt insbesondere, wenn von Ihnen fehlerhafte oder unvollständige Daten geliefert werden.

6.2 Leistungsausschluss

Die folgenden, für eine Zertifizierung erforderlichen Maßnahmen sind nicht Bestandteil des Angebots und können optional zusätzlich beauftragt werden:

- Audit Vor- und Nachbereitung
- Auditdurchführung (durch einen unabhängigen Dritten, sofern Vor- und Nachbereitung durch EnBW durchgeführt wurde)
- Analysieren der Schwachstellen auf Basis der Findings aus dem Audit
- Erstellung eines Maßnahmenkataloges
- Planung und Herstellung der Zertifizierungsreife
- Überprüfung der Wirksamkeit

6.3 Vertraulicher Umgang mit Daten

Die mit der Durchführung des Quick-Checks betrauten Mitarbeiter sind zum vertraulichen Umgang mit den Daten und Ergebnissen verpflichtet. Das Ergebnis wird vom Auftragnehmer ausschließlich dem Auftraggeber zur Verfügung gestellt.

7 Optionale Leistungen

7.1 Penetrationstests

EnBW FKS bietet Ihnen auf Wunsch an, die IT-Infrastruktur des Unternehmens mittels Penetrationstests zu evaluieren. Es werden mehrstufige, individuell angepasste Tests angeboten und gemäß Kundenwunsch durchgeführt. Wahlweise können bspw.

- Black-Box- oder
- White-Box-Verfahren

durchgeführt werden.

8 Preise und Konditionen

Unser Produkt FKS Quick-Check Ihrer IT-Infrastruktur zur Identifikation Ihrer relevantesten Risiken und entsprechende Maßnahmenvorschläge zur Behebung bieten wir Ihnen, für

3.459,00 Euro

an.

Reisezeiten und Reisekosten zu dem genannten Interview sind mit dem Angebotspreis abgegolten.
Werden zusätzlich Beratertagen beauftragt, sind Reisekosten Bestandteil des Tagessatzes. Reisezeiten werden innerhalb des Tagessatzes erbracht. Beratertage werden als kleinste Einheit mit einem halben Tag verrechnet. 1 Beratertag entspricht 8 Stunden.

Entstehen aufgrund von Nichtverfügbarkeiten wesentlicher Know-How-Träger in Ihrem Unternehmen zusätzliche Aufwände oder müssen - aus Gründen, die durch Ihr Unternehmen zu vertreten sind - zusätzliche Termine vereinbart werden, so werden diese Aufwände separat mit 1.300 € pro Tag á 8 Stunden in Rechnung gestellt und sind somit preislich nicht von diesem Angebot umfasst.

Weiterführende Leistungen werden nur nach Anweisung und Beauftragung durch den Auftraggeber erbracht.

Alle genannten Preise verstehen sich zuzüglich der zum Zeitpunkt der Leistungserbringung gültigen Mehrwertsteuer.

9 Anlage

AGB Geschäftsbereich „Systemkritische Infrastruktur“