Inhalt

Seite

Einleitung ... 3
1 Anwendungsbereich ... 4
2 Normative Verweisungen ... 4
3 Begriffe und Symbole ... 4
3.1 Begriffe ... 4
3.2 Abkürzungen und Akronyme ... 7
3.3 Konventionen ... 8
4 Anforderungen an Zonen, Conduits und Risikobeurteilungen ... 8
4.1 Überblick ... 8
4.2 ZCR-1: Identifizieren des zu berücksichtigenden Systems ... 10
4.2.1 ZCR-1.1: Identifizieren des SUC-Bereichs und der Zugangspunkte ... 10
4.3 ZCR-2: Erste Cybersicherheitsrisikobeurteilung ... 10
4.3.1 ZCR-2.1: Durchführen der ersten Cybersicherheitsrisikobeurteilung ... 10
4.4 ZCR-3: Aufteilung des SUC in Zonen und Kanäle ... 11
4.4.1 Überblick ... 11
4.4.2 ZCR-3.1: Zonen und Kanäle festlegen ... 11
4.4.3 ZCR-3.2: Separate Geschäfts- und Steuerungssystem-Anlagen ... 12
4.4.4 ZCR-3.3: Separate sicherheitsbezogene Anlagen ... 12
4.4.5 ZCR-3.4: Separate vorübergehend angeschlossene Geräte ... 12
4.4.6 ZCR-3.5: Separate kabellose Geräte ... 13
4.4.7 ZCR-3.6: Über externe Netzwerke verbundene separate Geräte ... 13
4.5 ZCR-4: Risikovergleich ... 13
4.5.1 ZCR-4.1: Vergleich zwischen allgemeinem und tolerierbarem Risiko ... 13
4.6 ZCR-5: Durchführen einer ausführlichen Cybersicherheitsrisikobeurteilung ... 13
4.6.1 Überblick ... 13
4.6.2 ZCR-5.1: Bedrohungen identifizieren ... 16
4.6.3 ZCR-5.2: Schwachstellen identifizieren ... 17
4.6.4 ZCR-5.3: Bestimmen der Konsequenz und Auswirkung ... 17
4.6.5 ZCR-5.4: Bestimmen der unverringerten Wahrscheinlichkeit ... 18
4.6.6 ZCR-5.5: Bestimmen des unverringerten Cybersicherheitsrisikos ... 18
4.6.7 ZCR-5.6: Bestimmen des Security-Level-Ziels (SL-T) ... 19
4.6.8 ZCR-5.7: Vergleich zwischen unverringertem und tolerierbarem Risiko ... 19
4.6.9 ZCR-5.8: Identifizieren und Bewerten bestehender Gegenmaßnahmen ... 19
4.6.10 ZCR-5.9: Neubewerten der Wahrscheinlichkeit und der Auswirkung ... 20
4.6.11 ZCR-5.10: Bestimmen des Restrisikos ... 20
4.6.12 ZCR-5.11: Vergleich zwischen dem Restrisiko und dem tolerierbaren Risiko ... 20
4.6.13 ZCR-5.12: Identifizieren zusätzlicher Cybersicherheitsgegenmaßnahmen ... 20

Seite

4.6.14 ZCR-5.13: Dokumentieren und Kommunizieren von Ergebnissen ... 21
4.7 ZCR-6: Dokumentieren von Cybersicherheitsanforderungen, -annahmen und -beschränkungen ... 21
4.7.1 Überblick ... 21
4.7.2 ZCR-6.1: Festlegung der Cybersicherheitsanforderungen ... 21
4.7.3 ZCR-6.2: SUC-Beschreibung ... 22
4.7.4 ZCR-6.3: Zonen- und Kanalzeichnungen ... 22
4.7.5 ZCR-6.4: Zonen- und Kanaleigenschaften ... 22
4.7.6 ZCR-6.5: Annahme zur Betriebsumgebung ... 24
4.7.7 ZCR-6.6: Bedrohungsumgebung ... 24
4.7.8 ZCR-6.7: IT-Sicherheitspolitik ... 25
4.7.9 ZCR-6.8: Tolerierbares Risiko ... 25
4.7.10 ZCR-6.9: Gesetzliche Anforderungen ... 25
4.8 ZCR-7: Genehmigung des Anlagenbetreibers ... 25
4.8.1 ZCR-7.1: Einholen der Genehmigung des Anlagenbetreibers ... 25
Anhang A (informativ) Security-Level ... 27
Anhang B (informativ) Risikomatrizen ... 28
Literaturhinweise ... 33

Bilder

Bild 1 – Arbeitsablauf zur Festlegung der Zonen und Kanäle und zur Beurteilung des Risikos ... 10
Bild 2 – Arbeitsablauf der ausführlichen Cybersicherheitsrisikobeurteilung je Zone oder Kanal ... 16
Bild 3 – Beispiel für eine 3 x 5 Risikomatrix ... 28
Bild 4 – Beispiel für eine Konsequenz- oder Schweregradskala ... 30
Bild 5 – Beispiel für eine einfache 3 x 3 Risikomatrix ... 31
Bild 6 – Beispiel für eine 5 x 5 Risikomatrix ... 31
Bild 7 – Beispiel für eine 3 x 4 Matrix ... 32

Tabellen

Tabelle 1 – Beispiel für eine Wahrscheinlichkeitsskala ... 29