

Anwendungsbeginn

Anwendungsbeginn dieses Dokuments ist 2019-03-01.

Inhalt

	Seite
Vorwort.....	8
Einleitung	9
1 Anwendungsbereich	10
2 Normative Verweisungen	12
3 Begriffe und Abkürzungen	12
3.1 Begriffe	13
3.2 Abkürzungen	18
4 Grundlagen	19
4.1 Allgemeines	19
4.2 Schutzziele	19
4.3 Informationssicherheitsmanagementsystem im Bereich der Straßenverkehrstechnik	20
4.3.1 Schützenswerte Informationswerte	20
4.3.2 Festlegung der Sicherheitsanforderungen	20
4.3.3 Einschätzung der Sicherheitsrisiken	20
4.3.4 Auswahl von Maßnahmen	21
4.4 Bedrohungslageanalyse für Systeme der Straßenverkehrstechnik	21
4.5 Risikobewertung	22
4.6 Risikobehandlung	23
5 Informationssicherheitsrichtlinien	24
5.1 Vorgaben der Leitung für Informationssicherheit	24
5.1.1 Informationssicherheitsrichtlinien	24
5.1.2 Überprüfung der Informationssicherheitsrichtlinien	24
6 Organisation der Informationssicherheit.....	24
6.1 Interne Organisation	24
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten	24
6.1.2 Aufgabentrennung	25
6.1.3 Kontakt mit Behörden	25
6.1.4 Kontakt mit speziellen Interessensgruppen	25
6.1.5 Informationssicherheit im Projektmanagement	26
6.2 Mobilgeräte und Telearbeit.....	26
6.2.1 Richtlinie zu Mobilgeräten	26
6.2.2 Telearbeit.....	26

	Seite
7	Personalsicherheit..... 27
7.1	Vor der Beschäftigung..... 27
7.1.1	Sicherheitsüberprüfung..... 27
7.1.2	Beschäftigungs- und Vertragsbedingungen..... 27
7.2	Während der Beschäftigung..... 27
7.2.1	Verantwortlichkeiten der Leitung..... 27
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung..... 27
7.2.3	Maßregelungsprozess..... 28
7.3	Beendigung und Änderung der Beschäftigung 28
7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung 28
8	Verwaltung der Werte 28
8.1	Verantwortlichkeit für Werte 28
8.1.1	Inventarisierung der Werte..... 28
8.1.2	Zuständigkeit für Werte 28
8.1.3	Zulässiger Gebrauch von Werten 29
8.1.4	Rückgabe von Werten..... 29
8.2	Informationsklassifizierung..... 29
8.2.1	Klassifizierung von Information 29
8.2.2	Kennzeichnung von Information 29
8.2.3	Handhabung von Werten 29
8.3	Handhabung von Datenträgern..... 29
8.3.1	Handhabung von Wechseldatenträgern 29
8.3.2	Entsorgung von Datenträgern..... 29
8.3.3	Transport von Datenträgern..... 30
9	Zugangssteuerung 30
9.1	Geschäftsanforderungen an die Zugangssteuerung..... 30
9.1.1	Zugangssteuerungsrichtlinie 30
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten 30
9.2	Benutzerzugangsverwaltung..... 31
9.2.1	Registrierung und Deregistrierung von Benutzern..... 31
9.2.2	Zuteilung von Benutzerzugängen 31
9.2.3	Verwaltung privilegierter Zugangsrechte 31
9.2.4	Verwaltung geheimer Authentisierungsinformation von Benutzern..... 31
9.2.5	Überprüfung von Benutzerzugangsrechten 32
9.2.6	Entzug oder Anpassung von Zugangsrechten..... 32
9.3	Benutzerverantwortlichkeiten 32
9.3.1	Gebrauch geheimer Authentisierungsinformation 32
9.4	Zugangssteuerung für Systeme und Anwendungen..... 32
9.4.1	Informationszugangsbeschränkung 32

	Seite
9.4.2 Sichere Anmeldeverfahren.....	33
9.4.3 System zur Verwaltung von Kennwörtern.....	33
9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten.....	33
9.4.5 Zugangssteuerung für Quellcode von Programmen.....	33
10 Kryptographie.....	33
10.1 Kryptographische Maßnahmen.....	33
10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen.....	33
10.1.2 Schlüsselverwaltung.....	33
11 Physische und umgebungsbezogene Sicherheit.....	34
11.1 Sicherheitsbereiche.....	34
11.1.1 Physische Sicherheitsperimeter.....	34
11.1.2 Physische Zutrittssteuerung.....	34
11.1.3 Sichern von Büros, Räumen und Einrichtungen.....	35
11.1.4 Schutz vor externen und umweltbedingten Bedrohungen.....	35
11.1.5 Arbeiten in Sicherheitsbereichen.....	35
11.1.6 Anlieferungs- und Ladebereiche.....	35
11.2 Geräte und Betriebsmittel.....	35
11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln.....	35
11.2.2 Versorgungseinrichtungen.....	35
11.2.3 Sicherheit der Verkabelung.....	36
11.2.4 Instandhaltung von Geräten und Betriebsmitteln.....	36
11.2.5 Entfernen von Werten.....	36
11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten.....	36
11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln.....	36
11.2.8 Unbeaufsichtigte Benutzergeräte.....	37
11.2.9 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	37
12 Betriebssicherheit.....	37
12.1 Betriebsabläufe und -verantwortlichkeiten.....	37
12.1.1 Dokumentierte Betriebsabläufe.....	37
12.1.2 Änderungssteuerung.....	37
12.1.3 Kapazitätssteuerung.....	37
12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....	38
12.2 Schutz vor Schadsoftware.....	38
12.2.1 Maßnahmen gegen Schadsoftware.....	38
12.3 Datensicherung.....	39
12.3.1 Sicherung von Information.....	39
12.4 Protokollierung und Überwachung.....	39
12.4.1 Ereignisprotokollierung.....	39
12.4.2 Schutz der Protokollinformation.....	40

	Seite
12.4.3 Administratoren- und Bedienerprotokolle.....	40
12.4.4 Uhrensynchronisation	40
12.5 Steuerung von Software im Betrieb	40
12.5.1 Installation von Software auf Systemen im Betrieb	40
12.6 Handhabung technischer Schwachstellen	40
12.6.1 Handhabung von technischen Schwachstellen	40
12.6.2 Einschränkungen von Softwareinstallation	41
12.7 Audits von Informationssystemen	41
12.7.1 Maßnahmen für Audits von Informationssystemen	41
13 Kommunikationssicherheit	41
13.1 Netzwerksicherheitsmanagement.....	41
13.1.1 Netzwerksteuerungsmaßnahmen	41
13.1.2 Sicherheit von Netzwerkdiensten.....	41
13.1.3 Trennung in Netzwerken	41
13.2 Informationsübertragung	42
13.2.1 Richtlinien und Verfahren für die Informationsübertragung	42
13.2.2 Vereinbarungen zur Informationsübertragung	42
13.2.3 Elektronische Nachrichtenübermittlung	42
13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	42
14 Anschaffung, Entwicklung und Instandhaltung von Systemen	42
14.1 Sicherheitsanforderungen an Informationssysteme.....	42
14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen	42
14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	43
14.1.3 Schutz der Transaktionen bei Anwendungsdiensten.....	43
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen	43
14.2.1 Richtlinie für sichere Entwicklung	43
14.2.2 Verfahren zur Verwaltung von Systemänderungen	43
14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	43
14.2.4 Beschränkung von Änderungen an Softwarepaketen	43
14.2.5 Grundsätze für Analyse, Entwicklung und Pflege sicherer Systeme	43
14.2.6 Sichere Entwicklungsumgebung.....	43
14.2.7 Ausgegliederte Entwicklung	43
14.2.8 Testen der Systemsicherheit.....	44
14.2.9 Systemabnahmetest	44
14.3 Testdaten	44
14.3.1 Schutz von Testdaten	44
15 Lieferantenbeziehungen.....	44
15.1 Informationssicherheit in Lieferantenbeziehungen	44
15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen.....	44

— Vornorm —

DIN VDE V 0832-700 (VDE V 0832-700):2019-03

	Seite
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen 44
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie 44
15.2	Steuerung der Dienstleistungserbringung von Lieferanten 45
15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen 45
15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen 45
16	Handhabung von Informationssicherheitsvorfällen 45
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen 45
16.1.1	Verantwortlichkeiten und Verfahren 45
16.1.2	Meldung von Informationssicherheitsereignissen 45
16.1.3	Meldung von Schwächen in der Informationssicherheit 45
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse 45
16.1.5	Reaktion auf Informationssicherheitsvorfälle 46
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen 46
16.1.7	Sammeln von Beweismaterial 46
17	Informationssicherheitsaspekte beim Business Continuity Management 46
17.1	Aufrechterhalten der Informationssicherheit 46
17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit 46
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit 46
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit 46
17.2	Redundanzen 46
17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen 46
18	Compliance 46
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen 46
18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen 46
18.1.2	Geistige Eigentumsrechte 46
18.1.3	Schutz von Aufzeichnungen 47
18.1.4	Privatsphäre und Schutz von personenbezogener Information 47
18.1.5	Regelungen bezüglich kryptographischer Maßnahmen 47
18.2	Überprüfungen der Informationssicherheit 47
18.2.1	Unabhängige Überprüfung der Informationssicherheit 47
18.2.2	Einhaltung von Sicherheitsrichtlinien und -standards 47
18.2.3	Überprüfung der Einhaltung von technischen Vorgaben 47
Anhang A (informativ) Beispielhafte Risikobewertung für typische Bedrohungen auf Systeme der Straßenverkehrstechnik zur Unterstützung der Betreiber 48	
Literaturhinweise 55	
Bilder	
Bild 1 – Beispiel für ein System aus dezentraler Straßenverkehrs-Signalanlage mit Peripheriekomponenten und Zentralsteuerung 11	
Bild 2 – Beispiel für eine dezentrale Streckenstation mit Schildern und Zentralsteuerung 11	

Tabellen

Tabelle 1 – Mögliche Schadensauswirkungen bei Bedrohungen für Systeme der Straßenverkehrstechnik	22
Tabelle 2 – Eintrittswahrscheinlichkeit von Risiken.....	22
Tabelle 3 – Anzahl der dezentralen Anlagen, die von einem Risiko betroffen sein können	22
Tabelle 4 – Potenzielle Schadensauswirkungen von Risiken	23
Tabelle 5 – Risikobewertung in Abhängigkeit von Schadensauswirkung, Anzahl der betroffenen dezentralen Anlagen und Eintrittswahrscheinlichkeit.....	24
Tabelle A.1 – Bedrohungen, die auf die Zentralsteuerung wirken können	49
Tabelle A.2 – Bedrohungen, die auf die Kommunikationssysteme wirken können	50
Tabelle A.3 – Bedrohungen, die auf die dezentralen Anlagen wirken können	51
Tabelle A.4 – Bedrohungen, die auf die Peripheriegeräte wirken können	52
Tabelle A.5 – Bedrohungen, die auf mobile Geräte für Servicezwecke wirken können	53
Tabelle A.6 – Bedrohungen, die auf alle Elemente von Straßenverkehrsanlagen wirken können	54