Anwendungsbeginn

Anwendungsbeginn der VDE-Anwendungsregel ist 2018-02-01.

Inhalt

Seite

Vorwort ... 5
Einleitung ... 6
1 Anwendungsbereich ... 7
2 Normative Verweisungen ... 7
3 Begriffe und Abkürzungen ... 7
3.1 Begriffe ... 7
3.2 Weitere Begriffe zum Datenschutz ... 10
3.3 Begriffe zur Architektur und zu Komponenten ... 14
3.4 Sicherheitsbegriffe zu technischen Systemen ... 14
3.5 Abkürzungen ... 15
4 Architektur ... 15
4.1 Betriebsumgebungen ... 15
4.2 Schutzzonen ... 16
4.3 IT-Sicherheitsarchitektur ... 16
4.3.1 Sicherheitsarchitekturvarianten ... 16
4.3.2 Sicherung der Kommunikation ... 16
4.3.3 Sicherung der Daten ... 17
5 Sicherheitsanforderungen (Security Requirements) ... 17
5.1 Schutzniveau ... 17
5.2 Identifikation und Authentifizierung ... 18
5.2.1 Motivation und Schutzniveaus für Identifikation und Authentifizierung ... 18
5.2.2 Nutzer Identifikation und Authentifizierung ... 19
5.2.3 Geräte-/Software-Prozess-Identifikation und -Authentifizierung ... 19
5.2.4 Stärke der Passwortbasierten Authentifizierung ... 20
5.2.5 Authentifizierung basierend auf Symmetrischen Verfahren ... 21
5.2.6 Authentifizierung basierend auf Asymmetrischen Schlüsseln ... 21
5.2.7 Authentifizierung basierend auf Asymmetrischen Schlüsseln mit Public Key Infrastruktur ... 22
5.2.8 Rückmeldung des Authentifizierers ... 22
5.2.9 Fehlerhafte Authentifizierungs Versuche ... 23
5.2.10 Zugriffsbenachrichtigung und Freigabe ... 23
5.3 Autorisierung und Nutzungskontrolle ... 23
5.3.1 Motivation und Schutzniveaus für Autorisierung und Nutzungskontrolle ... 23
5.3.2 Durchsetzung der Autorisierung ... 23
5.3.3 Nutzungskontrolle von Funkverbindungen ... 24
5.3.4 Nutzungskontrolle von tragbaren und mobilen Geräten ... 24

Seite

5.3.5 Plattformübergreifender Code 24
5.3.6 Sitzungssperrung 24
5.3.7 Auditierbare Ereignisse 24
5.3.8 Speicherkapazität für Audits 25
5.3.9 Reaktion auf Fehler bei der Erzeugung von Audits 25
5.3.10 Zeitstempel für Audits 25
5.3.11 Nicht-Abstreitbarkeit 25
5.4 System-Integrität 26
5.4.1 Motivation und Schutzniveaus für System-Integrität 26
5.4.2 Kommunikations-Integrität 27
5.4.3 Schutz vor Schadcode 27
5.4.4 Verifikation der IT-Sicherheitsfunktionalität 27
5.4.5 Software- und Informationsintegrität 28
5.4.6 Eingabevalidierung 28
5.4.7 Vorbestimmte Zustände der Ausgänge 28
5.4.8 Fehlerbehandlung 29
5.4.9 Sitzungsintegrität 29
5.4.10 Schutz von Prüfinformationen 29
5.5 Vertraulichkeit 29
5.5.1 Motivation und Schutzniveaus für Vertraulichkeit 29
5.5.2 Vertrauliche Kommunikation 30
5.5.3 Vertrauliche Verarbeitung 30
5.5.4 Vertrauliche Speicherung 30
5.5.5 Anonymisierung 31
5.5.6 Pseudonymisierung 31
5.6 Datenflusskontrolle 31
5.6.1 Motivation und Schutzniveaus für Segmentierung 31
5.6.2 Netzwerk Segmentierung 31
5.6.3 Schutz der Zonengrenzen 32
5.6.4 Partitionierung der Software 33
5.6.5 Datensparsamkeit und Zweckbindung 33
5.6.6 Intervenierbarkeit 33
5.6.7 Partitionierung personenbeziehbarer Daten 35
5.6.8 Nicht Verkettbarkeit 35
5.7 Bereitstellung von Ereignissen 36
5.7.1 Motivation und Schutzniveaus für Bereitstellung von Ereignissen 36
5.7.2 Zugriff auf System-Logs für sicherheitsrelevante Ereignisse 36
5.7.3 Kontinuierliche Überwachung der Schutzmaßnahmen 36
5.7.4 Transparenz über Datenflüsse 36

Seite
5.8 Verfügbarkeit von Ressourcen ... 37
5.8.1 Motivation und Schutzniveaus für die Verfügbarkeit von Ressourcen ... 37
5.8.2 Schutz gegen Denial of Service (DoS) ... 37
5.8.3 Ressourcenmanagement ... 38
5.8.4 Datensicherung (Backup) ... 38
5.8.5 Wiederherstellung ... 38
5.8.6 Notstromversorgung ... 39
5.8.7 Netz- und IT-Sicherheitseinstellung ... 39
5.8.8 Geringste Funktionalität ... 39
5.8.9 Verzeichnis der Schnittstellen des zu schützenden Systems ... 39
5.8.10 Verzeichnis der Kommunizierenden Komponenten des zu schützenden Systems ... 39
5.8.11 Autonomer Offline Betrieb ... 40
6 Risiken und Bedrohungen ... 40
6.1 Einleitung ... 40
6.2 Schützenswerte Güter (Assets) ... 40
6.2.1 Physische Angriffe ... 44
6.2.2 Unbeabsichtigte versehentliche Beeinträchtigungen ... 44
6.2.3 Katastrophen ... 44
6.3 Zerstörung oder Verlust (von IT Assets) ... 44
6.4 Fehler/Fehlfunktionen ... 44
6.5 Ausfälle ... 44
6.6 Belauschen, Abfangen, Übernahme ... 45
6.7 Missbrauch ... 45
6.8 Gesetzbruch ... 46
7 Organisatorische Empfehlungen für den Betrieb in Heim und Gebäude ... 46
Anhang A (informativ) Beziehung zwischen Schutzbedarf und Schutzniveau ... 47
Anhang B (informativ) Informierte elektronische zweckbasierte Einwilligung ... 48
B.1 Einleitung ... 48
B.2 Entwurf einer Zweckbeschreibung ... 50
B.3 Entwurf einer technischen Einwilligungserklärung ... 51
Literaturhinweise ... 52

Bilder

Bild 1 – Sicherheitsbegriffe für ein technisches System [VDE 2014] ... 14
Bild B.1 – Datenflüsse zur Information und Einwilligung ... 48

Tabellen

Tabelle B.1 – Voraussetzungen für eine wirksame informierte Einwilligung ... 48
Tabelle B.2 – Vorschlag für eine Zweckbeschreibung ... 50
Tabelle B.3 – Vorschlag einer technischen Einwilligungserklärung ... 51