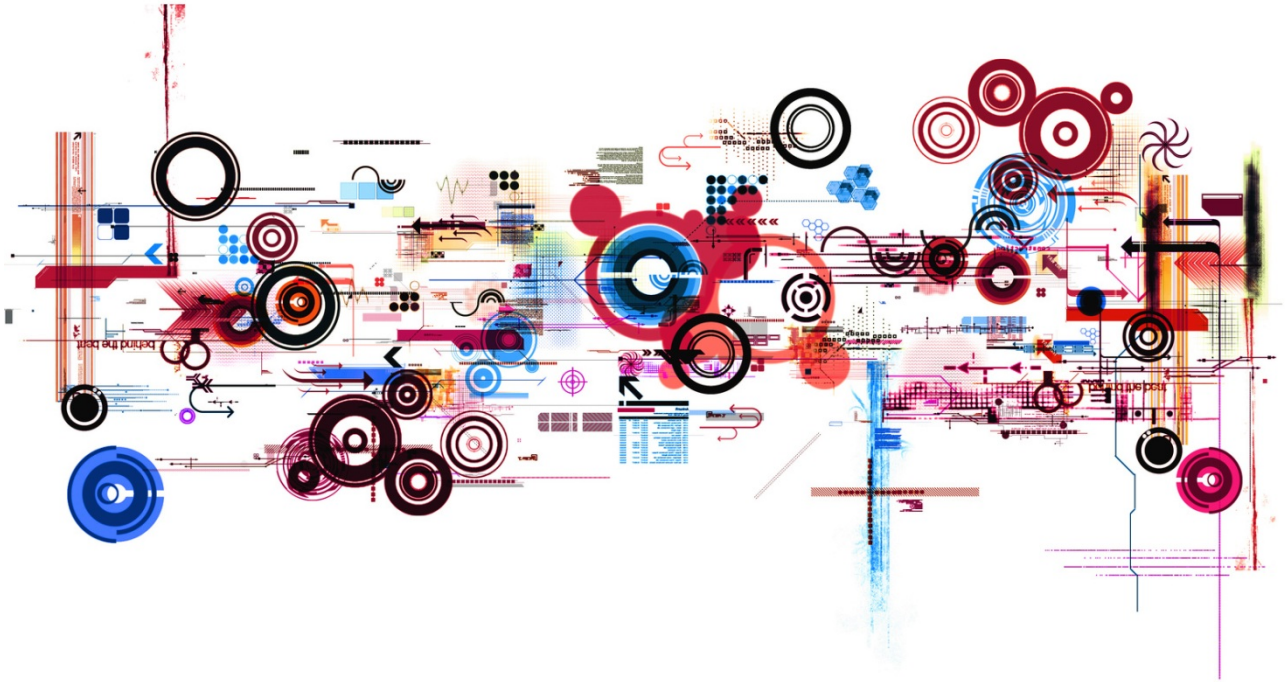
Sicherheitslücken in Embedded Systems

Die "vergessene Software": Risiken, Haftungsfragen und Vertragsgestaltung



Sicherheitslücken in Embedded Systems

- Das Embedded System – was ist das eigentlich?
- Softwaretypen in Embedded Systems
  - Proprietäre Software
  - Open Source Software
- Risiken – Die „vergessene“ Software und der Virus!
- Haftung – Was steuert meine Software eigentlich?
- Vertragsgestaltung – Es ist nicht alles nur Hardware!
  - Lizenz- und Haftungsfragen
  - Arbeitnehmererfindungsrecht
  - Verbindung zu anderen Systemen

Sicherheitslücken in Embedded Systems

- Das Embedded System – was ist das eigentlich?
- Softwaretypen in Embedded Systems
  - Proprietäre Software
  - Open Source Software
- Risiken – Die „vergessene“ Software und der Virus!
- Haftung – Was steuert meine Software eigentlich?
- Vertragsgestaltung – Es ist nicht alles nur Hardware!
  - Lizenz- und Haftungsfragen
  - Arbeitnehmererfindungsrecht
  - Verbindung zu anderen Systemen

Das Embedded System – was ist das eigentlich?

- Der Ausdruck eingebettetes System (auch engl. embedded system) bezeichnet eine elektronische Recheneinheit oder Computer (Datenverarbeitungseinheit), der in einen **technischen Kontext eingebunden** (eingebettet) ist. Dabei hat die Datenverarbeitungseinheit entweder die Aufgabe, das System, in das sie eingebettet ist, zu **steuern**, zu **regeln** oder zu **überwachen**. Oder die Datenverarbeitungseinheit ist für eine Form der **Daten- bzw. Signalverarbeitung** zuständig, beispielsweise beim Ver- bzw. Entschlüsseln, Codieren bzw. Decodieren oder Filtern.

- Oft werden eingebettete Systeme speziell an eine Aufgabe angepasst. Aus Kostengründen wird eine optimierte, **gemischte Hardware-Software-Implementierung** gewählt. Dabei vereinigt eine solche Konstruktion die große Flexibilität von Software mit der Leistungsfähigkeit der Hardware. Die Software dient dabei sowohl zur Steuerung des Systems selbst, als auch ggf. zur Interaktion des Systems mit der Außenwelt über definierte **Schnittstellen** oder **Protokolle** (z. B. LIN-Bus, CAN-Bus oder IP über Ethernet).

Das Embedded System – was ist das eigentlich?

ICE Leitstand mit integrierter Steuersoftware

Quelle Wikipedia, Autor: S. Terfloth, Creative Commons Lizenz

Das Embedded System – was ist das eigentlich?

Siemens Simatic Microbox PC 427B mit Betriebssystem Windows XP Embedded

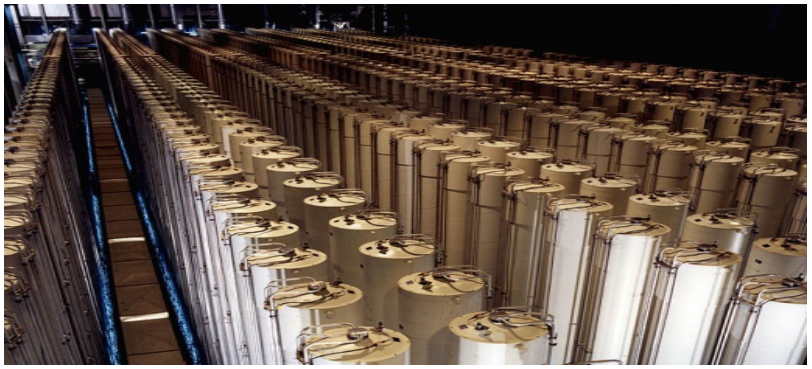
Quelle: Siemens I IA/DT-Bilddatenbank unter https://www.automation.siemens.com/bilddb/guiWelcome.asp

Das Embedded System – was ist das eigentlich?

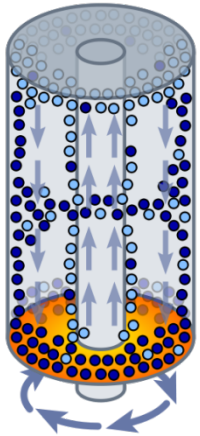
Bizerba Kassensysteme und Etikettier-Systeme

Quelle: http://www.bizerba-openworld.com

Das Embedded System – was ist das eigentlich?



Type	Original Machine	Deployment Period	Rotor characteristics				Separative Power
			Material	Speed	Diameter	Length	
	Zippe	1940s–50s	Aluminum	350 m/s	7.4 cm	0.3 m	0.44 SWU/yr
P-1	SNOR/CNOR	1960s–70s	Aluminum	350 m/s	10 cm	2.0 m	2–3 SWU/yr
P-2	G-2	1960s–70s	Maraging steel	485 m/s	15 cm	1.0 m	5–6 SWU/yr
P-3	4-M	Early 1980s	Maraging steel	(485 m/s)	n/a	2.0 m	12 SWU/yr
P-4	SLM (TC-10)	Late 1980s	Maraging steel	500 m/s	15 cm	3.2 m	21 SWU/yr
	TC-11	Late 1980s	Carbon fiber	(600 m/s)	n/a	(3.0 m)	n/a
	TC-12	1990s	Carbon fiber	(620 m/s)	(20 cm)	(3.0 m)	40 SWU/yr
	TC-21	2000s	Carbon fiber	(770 m/s)	(20 cm)	(5.0 m)	100 SWU/yr
	AC100	2000s	Carbon fiber	(900 m/s)	(60 cm)	(12.0 m)	330 SWU/yr



Zentrifugen

Quellen: Wikipedia, Cascade of gas centrifuges used to produce enriched uranium. U.S. gas centrifuge plant in Piketon, Ohio 1984, http://www.princeton.edu/~aglaser/2008aglaser_sgsvol16.pdf, http://en.wikipedia.org/wiki/Zippe-type_centrifuge,

Das Embedded System – was ist das eigentlich?

Steuerung eines Atomkraftwerkes (Kümmel)

Quelle: http://www.focus.de/digital/computer/chip-exklusiv/atomkraftwerke-stoerfall-software-update_aid_613985.html

Das Embedded System – was ist das eigentlich?

Embedded Systems im Haushalt

Quelle: Tauchcomputer Wikipedia, Autor: Thomei08 at Wikipedia, gemeinfrei, Fritzbox www.avm.de

Sicherheitslücken in Embedded Systems

- Das Embedded System – was ist das eigentlich?
- Softwaretypen in Embedded Systems
  - Proprietäre Software
  - Open Source Software
- Risiken – Die „vergessene“ Software und der Virus!
- Haftung – Was steuert meine Software eigentlich?
- Vertragsgestaltung – Es ist nicht alles nur Hardware!
  - Lizenz- und Haftungsfragen
  - Arbeitnehmererfindungsrecht
  - Verbindung zu anderen Systemen

Softwaretypen in Embedded Systems

- Geräteimmanente Standard-Software wie BIOS (z.B. AMIBIOS) oder spezielle Betriebssysteme (z.B. Windows XP Embedded, IOS – Cisco Router Betriebssysteme)
- Spezialentwicklungen für Branchenlösungen (ProOSEK und RTA-OSEK für den Automotive-Bereich, POS und QNX als Firmenlösungen)
- „Unbekannte“ Software in „Black Box“ Lösungen (z.B. Tauchcomputer, RMOS2 Statisches Echtzeit-Betriebssystem der Siemens AG)

Softwaretypen in Embedded Systems

- Bei der Prüfung von Erfindungen, die Merkmale technischer Natur mit Merkmalen nichttechnischer Art verknüpfen, auf erfinderische Tätigkeit muss der genannte Erfindungs-gegenstand unter Einschluss der etwaigen Rechenregel berücksichtigt werden. Es darf der Erfindungsgegenstand nicht zerlegt und dann nur der Teil der Erfindung auf erfinderische Tätigkeit, d. h. Naheliegen, geprüft werden, der aus den technischen Merkmalen besteht.
- Enthält eine Erfindung technische und nichttechnische Merkmale, so ist bei deren Prüfung auf erfinderische Tätigkeit der gesamte Erfindungsgegenstand unter Einschluss einer etwaigen Rechenregel zu berücksichtigen.
- BGH, Urt.v. 4.2.1992 - X ZR 43/91 (BPatG), Tauchcomputer

Softwaretypen in Embedded Systems

- OSEK = industrielles Standardisierungsgremium und bedeutet ausgeschrieben "**O**ffene Systeme und deren **S**chnittstellen für die **E**lektronik im **K**raftfahrzeug„

- Wesentliche Teile der OSEK/VDX-Spezifikationen wurden in die ISO-Norm 17356 überführt.
- OSEK-OIL = OSEK Implementation Language. In dieser Sprache werden Betriebssystemobjekte angelegt und beschrieben, wie z.B. Tasks, Interrupts, Ressourcen und Alarme. OIL bietet eine normierte Möglichkeit, für eine Applikation erforderliche Betriebssystemdienste zu beschreiben.
- OSEK-NM beschreibt unter anderem, wann sich Steuergeräte innerhalb eines Autos abschalten dürfen. NM steht dabei für Network Management; OSEK-NM ist dabei für alle Aufgaben zuständig, die sich mit der Verwaltung des Netzwerkes, das die Controller verbindet, beschäftigen.

Softwaretypen in Embedded Systems

- Linux basierte Betriebssysteme auf Open Source Basis (z.B. BlueCat Linux, ChorusOS, RTAI Linux Echtzeitsystem, Inferno)
- viele verschiedene Lizenztypen im Einsatz (z.B. GNU General Public License (GPL), GNU Lesser General Public License (LGPL), MIT-template, Lucent Public License 1.02, FreeType)
- **Achtung!**

  Teilweise Auswahlmöglichkeit unter verschiedenen offenen oder proprietären Lizenzmodellen (z.B. Inferno Operating System)

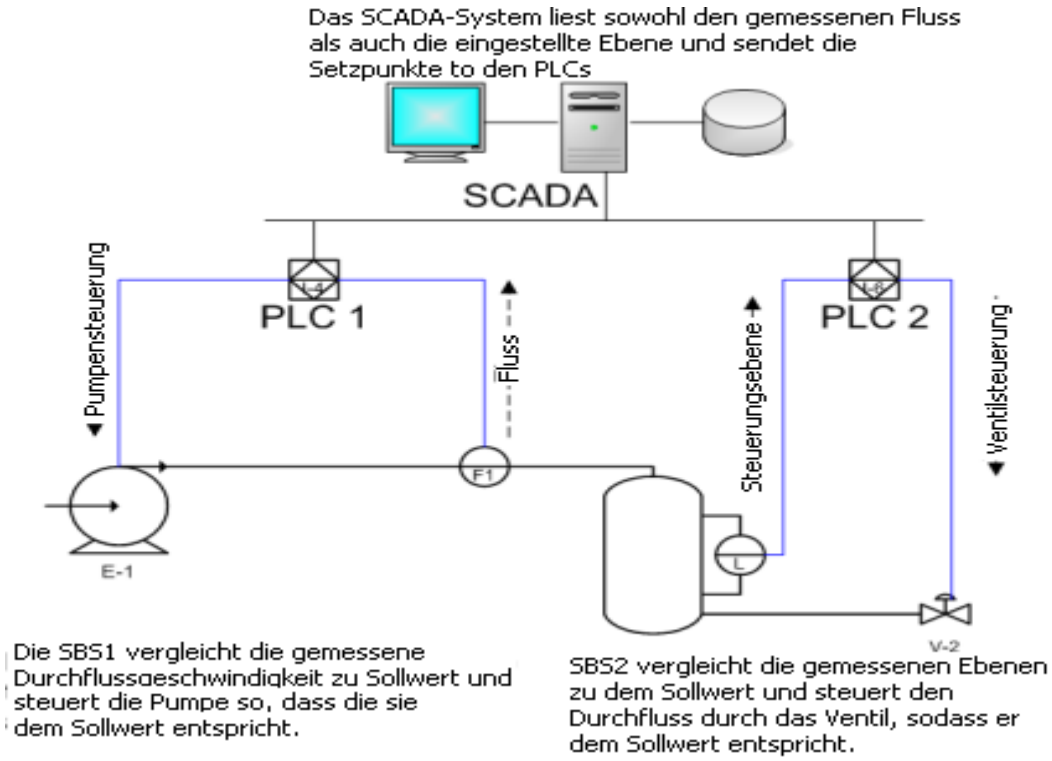
Praktische Relevanz?

- Rechtsstreit vor dem Landgericht Berlin zwischen dem Vertreiber von DSL-Routern AVM Computersysteme Vertriebs GmbH (AVM) und die Cybits AG (Cybits), ein Hersteller von Filterungssoftware für Kinder. **Beide Firmen benutzen den Linuxkernel**, der unter der GNU General Public License Version 2 (GNU GPL) steht, die jedermann das Recht gibt, die Software zu verwenden, zu verstehen (analysieren), zu verteilen (verbreiten) und zu verbessern (bearbeiten).
- Der Fall wurde von AVM mit dem Antrag eingeleitet, Cybits davon abzuhalten jegliche Teile der Firmware zu ändern, die in den Routern von AVM Verwendung finden, einschließlich des Linuxkernels. Das entsprechende Urteil des Kammergerichts Berlin (Urteil vom 06.09.2010, Az.: 24 U 71/10, Download: http://fsfe.org/projects/ftf/kg-avm-vs-cybits.pdf) verbietet den Vertrieb der Software von Cybits insoweit, als damit Fehlfunktionen bei der FritzBox ausgelöst werden, die dem Hersteller zugerechnet werden könnten. Dies stelle ein wettbewerbswidriges Verhalten dar, das gem. § 3 Abs. 1 UWG verboten sei.

Sicherheitslücken in Embedded Systems

- Das Embedded System – was ist das eigentlich?
- Softwaretypen in Embedded Systems
  - Proprietäre Software
  - Open Source Software
- Risiken – Die „vergessene“ Software und der Virus!
- Haftung – Was steuert meine Software eigentlich?
- Vertragsgestaltung – Es ist nicht alles nur Hardware!
  - Lizenz- und Haftungsfragen
  - Arbeitnehmererfindungsrecht
  - Verbindung zu anderen Systemen

Beispiel SCADA System



Schematische Darstellung eines SCADA-Systems

Quelle: Englische Wikipedia |Urheber = W:en:user:HaPi |Datum = 2009-02-06 |Genehmigung = Public Domain-Lizenz der englischen Wikipedia

Beispiele

Siemens Simatic Microbox PC 427B mit Betriebssystem Windows XP Embedded

Quelle: Siemens I IA/DT-Bilddatenbank unter https://www.automation.siemens.com/bilddb/guiWelcome.asp

Die „vergessene“ Software und der Virus!

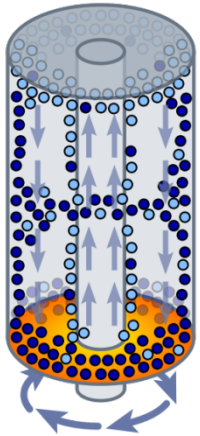
- Supervisory Control and Data Acquisition (**SCADA**) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.
- Die Kommunikation innerhalb von SCADA-Systemen erfolgt heute mehr und mehr auf der Basis von **TCP-basierten Internettechniken**.
- Stuxnet greift über die Betriebssystemsoftware auf die SCADA Systeme zu und gilt aufgrund seiner Komplexität und des Ziels, Steuerungssysteme von Industrieanlagen zu sabotieren, als bisher einzigartig.

Was ist eigentlich das Stuxnet Risiko?

900 Meter / Sekunde
=
3240 Kilometer pro Stunde

Concorde = 2150 km/h

Type	Original Machine	Deployment Period	Rotor characteristics				Separative Power
			Material	Speed	Diameter	Length	
	Zippe	1940s–50s	Aluminum	350 m/s	7.4 cm	0.3 m	0.44 SWU/yr
P-1	SNOR/CNOR	1960s–70s	Aluminum	350 m/s	10 cm	2.0 m	2–3 SWU/yr
P-2	G-2	1960s–70s	Maraging steel	485 m/s	15 cm	1.0 m	5–6 SWU/yr
P-3	4-M	Early 1980s	Maraging steel	(485 m/s)	n/a	2.0 m	12 SWU/yr
P-4	SLM (TC-10)	Late 1980s	Maraging steel	500 m/s	15 cm	3.2 m	21 SWU/yr
	TC-11	Late 1980s	Carbon fiber	(600 m/s)	n/a	(3.0 m)	n/a
	TC-12	1990s	Carbon fiber	(620 m/s)	(20 cm)	(3.0 m)	40 SWU/yr
	TC-21	2000s	Carbon fiber	(770 m/s)	(20 cm)	(5.0 m)	100 SWU/yr
	AC100	2000s	Carbon fiber	(900 m/s)	(60 cm)	(12.0 m)	330 SWU/yr



Zentrifugen

Quellen: Wikipedia, Cascade of gas centrifuges used to produce enriched uranium. U.S. gas centrifuge plant in Piketon, Ohio 1984, http://www.princeton.edu/~aglaser/2008aglaser_sgsvol16.pdf, http://en.wikipedia.org/wiki/Zippe-type_centrifuge,

Sicherheitslücken in Embedded Systems

- Das Embedded System – was ist das eigentlich?
- Softwaretypen in Embedded Systems
  - Proprietäre Software
  - Open Source Software
- Risiken – Die „vergessene“ Software und der Virus!
- Haftung – Was steuert meine Software eigentlich?
- Vertragsgestaltung – Es ist nicht alles nur Hardware!
  - Lizenz- und Haftungsfragen
  - Arbeitnehmererfindungsrecht
  - Verbindung zu anderen Systemen

Absicherung von Risiken? Haftungsausschlüsse?

- Anwendbarkeit des Grundprinzips von § 309 Ziffer 7 BGB über § 310 BGB auch im kaufmännischen Verkehr?
- Unabdingbarkeit der Ersatzansprüche bei Vorsatz und aus Produkthaftung nach § 14 ProdHaftG (Gesetz über die Haftung für fehlerhafte Produkte)
- Nur eingeschränkte Haftungsausschlüsse bei grober Fahrlässigkeit.
- Versicherungsausschluss in Betriebshaftpflichtbedingungen zum Beispiel für Produkthaftpflichtschäden, Schäden im Zusammenhang mit energiereichen ionisierenden Strahlen (insbesondere Atomkraft), Anlagen nach dem Wasserhaushaltsgesetz, dem Umwelthaftungsgesetz sowie nach der Richtlinie 2004/35/EG des europäischen Rates und des Parlaments vom 21. April 2004 über Umwelthaftung zur Vermeidung und Sanierung von Umweltschäden

Beispiel Windkraftanlage

- Die SWT-3.6-107 Windenergieanlage ist mit einem WebWPS SCADA-System ausgestattet. Dieses Anlagenfernüberwachungssystem bietet Kontrolle und Überwachung der Anlage über eine Vielzahl von Momentanwerten. Hierzu gehören elektrische und mechanische Daten, Betriebs- und Fehlermeldungen, meteorologische und netzspezifische Daten. Auswertungen können über einen **Standard-Internet-Browser** durchgeführt werden.
- Zusätzlich zum WebWPS SCADA-System wird die Windenergieanlage mit einem webbasierten Turbine Condition Monitoring (TCM) System ausgestattet. Auswertungen, detaillierte **Untersuchungen und Programmierung** können über einen **Standard-Internet-Browser** ausgeführt werden.
- Quelle: http://www.energy.siemens.com/hq/de/stromerzeugung/erneuerbare-energien/windenergie/windenergieanlagen/swt-3-6-107.htm

Beispiel Windkraftanlage – Sabotage?

Betriebsdaten

•Einschaltwindgeschwindigkeit 3-5 m/s

•Nenngeschwindigkeit bei ca. 13-14 m/s

•Abschaltwindgeschwindigkeit 25 m/s (schwerer Sturm, Windstärke 10)

•Überlebenswindgeschwindigkeit (Orkan/Windstärke 12 ab 32,7 m/s)

- 55 m/s (Standardausführung)
- 70 m/s (Sonderausführung).

•Die Spannungs- und Frequenzüberwachung sowie netzrelevante Einstellungen können über das Anlagenfernüberwachungssystem (WebWPS SCADA-System) vorgenommen werden.

Sicherheitslücken in Embedded Systems

- Das Embedded System – was ist das eigentlich?
- Softwaretypen in Embedded Systems
  - Proprietäre Software
  - Open Source Software
- Risiken – Die „vergessene“ Software und der Virus!
- Haftung – Was steuert meine Software eigentlich?
- Vertragsgestaltung – Es ist nicht alles nur Hardware!
  - Lizenz- und Haftungsfragen
  - Arbeitnehmererfindungsrecht
  - Verbindung zu anderen Systemen

Gestaltungshinweis Lizenzfragen

- Üblicherweise Einheitlichkeit des Entwicklungs- oder Erwerbsvertrages im Hinblick auf Hard- und Software .
- Prüfung ob Hard- oder Software überwiegt oder ein „Black Box“ System vorliegt.
- Jedenfalls: Einbindung von eigenen oder fremden „Lizenzbedingungen“ für die Embedded Software.
- Reiner Verweis auf Drittlizenzbedingungen nicht ausreichend.
- Soweit Updatefähigkeit gegeben, Regelungen für Softwareupdates der Embedded Software aufnehmen. Besonderheit sind dabei „Black Box“ Systeme, bei denen der Kunde auf die Software nicht zugreifen kann.

Mängelhaftung und Haftungsfragen

- Nacherfüllung bei hoch integrierten Systemen oft nur durch Komplettaustausch möglich.
- Wahlrecht des Anbieters im Hinblick auf die Rangfolge der Mängelrechte aufnehmen: z.B. zunächst Nachbesserung, dann Nacherfüllung und erst dann Minderung/Rücktritt. Beschränkung auf Nacherfüllung jedoch gemäß § 309 Nr. 8b bb) unzulässig.
- Regelung über Ein- und Ausbau bei Austausch aufnehmen; z.B. Mitwirkungspflichten, System-Downtimes
- Soweit Netzanbindung vorgesehen oder möglich, Nachbesserung durch Fernzugriff einräumen lassen.

Grundlagen Arbeitnehmererfindungsrecht

- Eine Arbeitnehmererfindung (Diensterfindung) ist eine patent- oder gebrauchsmusterfähige Erfindung, die ein Arbeitnehmer im Rahmen seiner Dienstpflicht geschaffen hat.
- Technische Verbesserungsvorschläge sind schöpferische Leistungen von Arbeitnehmern, die nicht patentierbar oder sonst schutzrechtsfähig sind, aber die Leistungsfähigkeit eines Unternehmens verbessern.
- Bei Inanspruchnahme einer Diensterfindung oder technischen Verbesserung, gehen alle vermögenswerten Rechte an der Diensterfindung auf den Arbeitgeber über, der im Gegenzug zu einem einen Anspruch auf angemessene Vergütung führt, sobald der Arbeitgeber die Diensterfindung in Anspruch genommen hat.

Gestaltungshinweis Arbeitnehmererfindungen

- In den Erstellungs- oder Überlassungsvertrag aufnehmen, wer die Kosten für die Arbeitnehmererfindung trägt.
  - Formulierungsbeispiel: „*Etwaige Vergütungen an Mitarbeiter des Auftragnehmers nach dem Arbeitnehmererfindungsgesetz trägt der Auftraggeber*."
- Im Unternehmen auf formelle Einhaltung der Regelungen des Arbeitnehmererfindungsgesetzes achten:
  - Meldepflicht des Arbeitnehmers mit genauen Angaben zur Erfindung
  - Ganz oder teilweise Inanspruchnahme-Erklärung des Arbeitgebers

Verbindung zu anderen Systemen

- Anforderungen z.B. des BSI Grundschutzhandbuches oder besonderer Regelungen des BSI als Mindestanforderung an die Netzsicherheit (z.B. § 21g EnWG i.V.m. § 21i Abs. 2 Ziffer 9 EnWG; BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents für die Passlesegeräte)
- Notwendige Maßnahmen nach Ziffer 4 der Anlage zu § 9 Satz 1 BDSG
- Vorgaben für technische Schutzmaßnahmen nach § 109 TKG
- Vorgaben von § 17 SigG und § 2 i.V.m § 15 SignV

Verbindung zu anderen Systemen

- Datenschutzregelungen in § 21g EnWG 2011
- Schutz von Daten aus dem Messsystem oder mit Hilfe des Messsystems erhobener Daten – auch Rücksicht auf Datenströme aus Ladestationen für Elektroautos inklusive Ladestellen-Roaming
- § 21d EnWG 2011 erweiterte Definition von Messsystemen: Messsysteme sind alle in ein Kommunikationsnetz eingebundenen Messeinrichtungen zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt.
- Eigenschaften und Funktionalitäten von Messsystemen sowie von Speicher- und Verarbeitungsmedien sind datenschutzgerecht zu regeln.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT !

FÜR RÜCKFRAGEN

ANWALTSCONTOR

RECHTSANWALT CHRISTIAN R. KAST
WWW.ANWALTSCONTOR.DE