Vorlesung Technikrecht
Cybersecurity

Prof. Dr. Ruth Janal, LL.M.

1

Prinzipien der IT-Sicherheit

Verfügbarkeit	• Die vorgesehen Verwendung von Informationen und Systemen darf nicht behindert werden
Integrität	• Korrektheit der Daten (Datenintegrität) und korrekte Funktionsweise des Systems (Systemintegrität).
Authentizität	• Die erhaltenen Daten stammen auch tatsächlich von der authentisierten Instanz
Vertraulichkeit	• Informationen dürfen nicht Unberechtigten zur Kenntnis gelangen

2

Beispiel WannaCry Ransomware

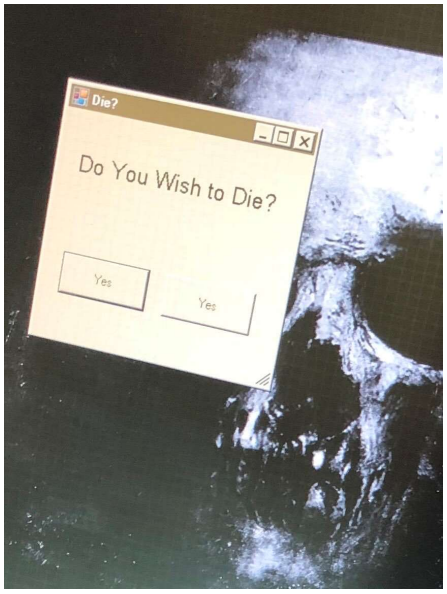
Quelle: dpa/P. Götzelt

3

Beispiel Jeep Cherokee

Quelle: Wired, https://www.youtube.com/watch?v=MK0SrxBC1xs

4

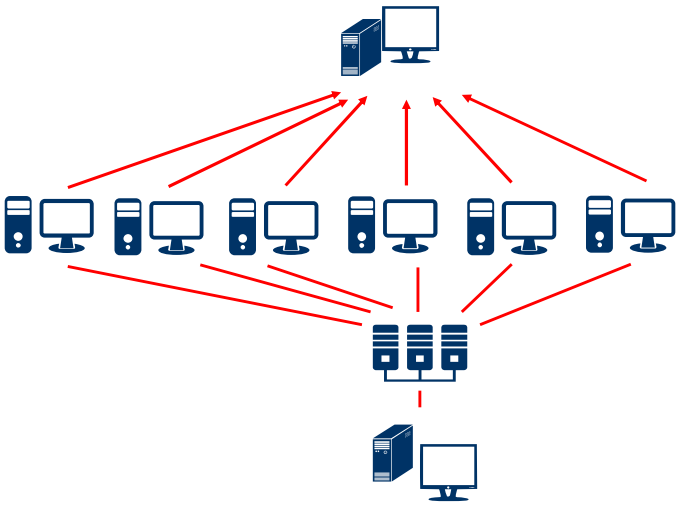


Beispiel
Medtronic Herzschrittmacher

(Demo von *Billy Rios* auf der BlackHat USA)

5

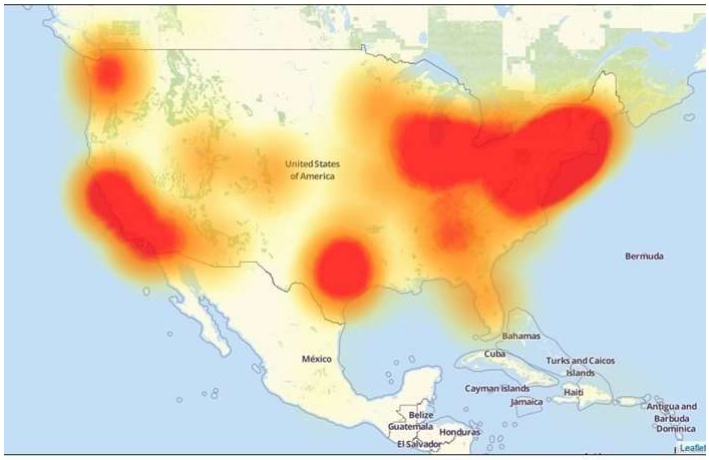
Distributed Denial of Service (DDoS)



6

Prof. Dr. Ruth Janal, LL.M.

Beispiel Dyn DDoS-Attacke



Quelle: Down Detector, https://de.wikipedia.org/wiki/DDoS-Angriffe_auf_Dyn

7

Prof. Dr. Ruth Janal, LL.M.

Schadensszenarien im Angriffsfall

unmittelbare Attacke

Angriff auf den **Nutzer** der Software

- Ausspähen, Veröffentlichen oder Löschen von Daten
- Fernsteuerung vernetzter Geräte
- Erpressung (Ransomware)
- etc.

mittelbare Attacke

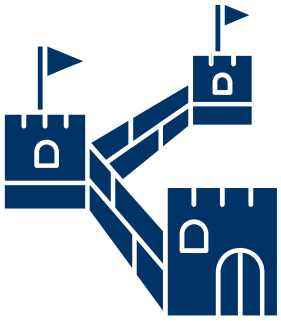
Angriff auf **Dritte** durch Bot-Netze

- DDoS-Angriffe
- Spam

8

Eigenschutz der Software- / Gerätenutzer

- für Private kaum möglich
- auch für gewerbliche Nutzer nur sehr eingeschränkt realisierbar



→ **Effektivste Lösung: Anforderungen an Softwareanbieter**

9

Vorlesung Technikrecht
Cybersecurity: Produktsicherheits- und Produkthaftungsrecht

Prof. Dr. Ruth Janal, LL.M.

10

Samsung beseitigt seit 2014 vorhandene, kritische Smartphone-Schwachstelle

Ein Forscher hat eine via MMS ausnutzbare Schwachstelle entdeckt, die seiner Einschätzung nach alle Android-Smartphones von Samsung seit 2014 betrifft.

Lesezeit: 1 Min. In Pocket speichern 35

Update verfügbar – wenn möglich zeitnah einspielen

Samsung hat die Schwachstelle im Zuge seines Mai-Updates gepatcht. In Samsungs ausführlichem Advisory zu den Updates wird die Lücke statt mit der CVE-Nummer mit der internen Bezeichnung SVE-2020-16747 aufgeführt.

Welche Geräte das Mai-Update erhalten (und zu welchem Zeitpunkt) , geht aus dem Advisory nicht konkret hervor: Samsung schreibt lediglich, dass die wichtigsten "Flaggschiff-Modelle" es im Zuge des monatlichen "Security Maintenance Release (SMR)"-Prozesses bekommen.

Eine separate Übersicht über die Update-Zyklen von Samsungs Android-Geräten legt die Vermutung nahe, dass einige Geräte das betreffende Update erst später (im Rahmen eines vierteljährlichen Zyklus) erhalten. heise Security hat diesbezüglich bei Samsung nachgefragt; die Antwort steht jedoch noch aus.

Quelle: https://heise.de/-4716443 v. 7.5.2020

11

Produktverantwortung

Produktsicherheit

- Wirtschaftsverwaltungsrecht
- Sicherheit ex ante
- Regulierung mit selbstregulativen Elementen
- hohe Bedeutung technischer Normen

Produkthaftung

- Zivilrecht
- Haftung ex post
- Berücksichtigung technischer Normen möglich
- Einhaltung der produkt-sicherheitsrechtlichen Anforderungen befreit nicht notwendigerweise von der Haftung

12

Medizinproduktegesetz

§ 3 Begriffsbestimmungen

1. Medizinprodukte sind alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, **Software**, Stoffe und Zubereitungen aus Stoffen oder andere Gegenstände einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten **Software**, die vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke
   a) der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
   b) der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
   c) der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder
   d) der Empfängnisregelung

   zu dienen bestimmt sind und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologisch oder immunologisch wirkende Mittel noch durch Metabolismus erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann.

13

ProduktSG – Grundstrukturen

Bereitstellung (§ 2 Nr. 4) eines Produkts (§ 2 Nr. 22) auf dem Markt
auch Ausstellung (§ 2 Nr. 2) und Inverkehrbringen (§ 2 Nr. 15)

Kein Verbraucherprodukt:

§ 3: allgemeine Anforderungen

Verbraucherprodukt:

§ 3

§ 6: zusätzliche Anforderungen

Harmonisierter Bereich, § 3 I
- Prinzip: keine Gefahr für Sicherheit & Gesundheit von Personen
- Anforderungen aus ProdSVen = umgesetzte EU-RL

↑ ↑ ↑
Vermutungswirkung harmonisierter Normen, § 4 II

Sonstige Produkte, § 3 II
- Prinzip: keine Gefahr für Sicherheit & Gesundheit von Personen
- Kriterien in § 3 II 2 und 3

↑ ↑ ↑
Vermutungswirkung harmonisierter und nationaler Normen, § 5 II

14

Produktsicherheitsgesetz

§ 2 Nr. 22 ProdSG

„Im Sinne dieses Gesetzes […] sind Produkte Waren, Stoffe oder Zubereitungen, die durch einen Fertigungsprozess hergestellt worden sind."

15

ProduktSG – Grundstrukturen

Bereitstellung (§ 2 Nr. 4) eines Produkts (§ 2 Nr. 22) auf dem Markt
auch Ausstellung (§ 2 Nr. 2) und Inverkehrbringen (§ 2 Nr. 15)

Kein Verbraucherprodukt:

§ 3: allgemeine Anforderungen

Harmonisierter Bereich, § 3 I
- Prinzip: keine Gefahr für Sicherheit & Gesundheit von Personen
- Anforderungen aus ProdSVen = umgesetzte EU-RL

Vermutungswirkung harmonisierter Normen, § 4 II

Verbraucherprodukt:

§ 3

§ 6: zusätzliche Anforderungen

Sonstige Produkte, § 3 II
- Prinzip: keine Gefahr für Sicherheit & Gesundheit von Personen
- Kriterien in § 3 II 2 und 3

Vermutungswirkung harmonisierter und nationaler Normen, § 5 II

16

Prof. Dr. Ruth Janal, LL.M.

Marktüberwachung

Allgemeine Marktüberwachung

- begründeter Verdacht, dass Produkt nicht die Sicherheitsanforderungen nach §§ 2-8 erfüllt:
- Maßnahmen nach § 26 II, z.B. Untersagen des Bereitstellens auf dem Markt, Anordnung der Überprüfung durch eine geeignete Prüfstelle, Anordnung von Rücknahme oder Rückruf, Warnhinweise; Sicherstellung, Vernichtung oder Unbrauchbarmachen von Produkten
- Pflichtgemäßes Ermessen („sind befugt“)
- Verhältnismäßigkeitsgrundsatz

Adressaten:
§§ 27, 2 Nr. 3, Nr. 29

Besondere Marktüberwachung

- Ernstes Risiko für Sicherheit & Gesundheit von Personen:
- Maßnahmen nach § 26 IV: Rückruf oder Rücknahme, Verbot des Bereitstellens
- Gebundene Entscheidung („haben zu untersagen“)
- RAPEX-Meldung, § 30

17

Bsp. „gefräßiger“ Staubsaugerroboter

Quelle: Yonhap/AAPIMAGE

18

Prof. Dr. Ruth Janal, LL.M.

Probleme bei der Anwendung des ProdSG

Software ist kein "Produkt"
- Allerdings ist embedded software Teil eines Produkts

Schutzzweck: Sicherheit und Gesundheit von Personen
- nicht: Daten, Vermögen, Persönlichkeitsrechte

Update-Pflicht problematisch
- Vorbehalt der wirtschaftlichen Zumutbarkeit
- Geschlossene Systeme und fehlende Speicherkapazitäten
- Update-Vornahme durch Nutzer fraglich

19

Produktverantwortung

Produktsicherheit

- Wirtschaftsverwaltungsrecht
- Sicherheit ex ante
- Regulierung mit selbstregulativen Elementen
- hohe Bedeutung technischer Normen

Produkthaftung

- Zivilrecht
- Haftung ex post
- Berücksichtigung technischer Normen möglich
- Einhaltung der produkt-sicherheitsrechtlichen Anforderungen befreit nicht notwendigerweise von der Haftung

20

Prof. Dr. Ruth Janal, LL.M.

Produktfehler:
Verkäufer vs. Hersteller als Anspruchsgegner

Verkäufer

Haftung aus Vertrag

- Äquivalenz- und Integritätsinteresse
- keine Haftung für Fehlverhalten des Herstellers

Haftung aus Delikt

- Schutz nur des Integritätsinteresses
- grds. keine Verkehrssicherungspflicht bzgl. der Qualität des Produkts
- Haftung für Produktfehler nur, falls Verkäufer = Hersteller iSd § 4 ProdHG

Hersteller

Haftung aus Vertrag (-)

Haftung aus Delikt

- Schutz nur des Integritätsinteresses
- § 823 I BGB bei Verletzung einer Verkehrssicherungspflicht
- § 1 ProdHG für Produktfehler

21

Prof. Dr. Ruth Janal, LL.M.

Digitale Inhalte-RL (noch nicht umgesetzt)

Art. 8 Abs. 2

Der Unternehmer stellt sicher, dass der Verbraucher über Aktualisierungen, einschließlich Sicherheitsaktualisierungen, die für den Erhalt der Vertragsmäßigkeit der digitalen Inhalte und digitalen Dienstleistungen erforderlich sind, informiert wird und dass diese ihm bereitgestellt werden, und zwar während des **Zeitraums**,

a) in dem die digitalen Inhalte oder digitalen Dienstleistungen im Rahmen des Vertrags bereitzustellen sind, wenn der Vertrag eine **fortlaufende Bereitstellung über einen Zeitraum** vorsieht, oder

b) den der Verbraucher aufgrund der Art und des Zwecks der digitalen Inhalte oder digitale Dienstleistungen und unter Berücksichtigung der Umstände und der Art des Vertrags **vernünftigerweise erwarten kann**, wenn der Vertrag eine einmalige Bereitstellung oder eine Reihe einzelner Bereitstellungen vorsieht.

(ähnliche Regelung in Art. 7 Abs. 3 Warenkauf-RL)

22

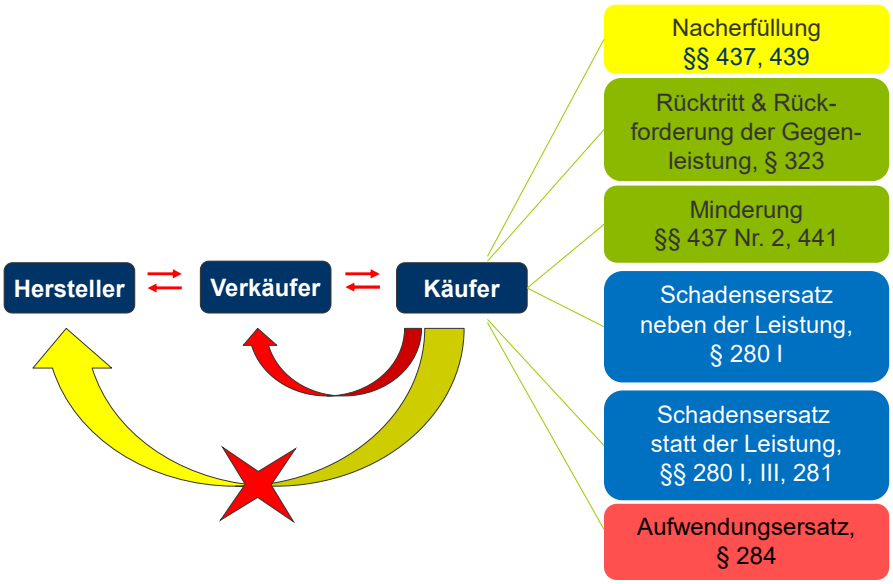
Digitale Inhalte-RL (noch nicht in Kraft)

Erwägungsgrund 47

Während des Zeitraums, den der Verbraucher vernünftigerweise erwarten würde, sollte der Unternehmer dem Verbraucher Aktualisierungen, einschließlich Sicherheitsaktualisierungen, bereitstellen, damit die digitalen Inhalte oder digitalen Dienstleistungen in vertragsgemäßem Zustand bleiben und sicher bleiben. So sollte beispielsweise in Bezug auf digitale Inhalte oder digitale Dienstleistungen, deren Zweck zeitlich begrenzt ist, die Verpflichtung zur Bereitstellung von Aktualisierungen auf diesen begrenzten Zeitraum beschränkt sein, **während bei anderen Arten digitaler Inhalte oder digitaler Dienstleistungen der Zeitraum, in dem dem Verbraucher Aktualisierungen bereitgestellt werden sollten, dem Gewährleistungszeitraum für Vertragswidrigkeit entsprechen könnte oder über diesen Zeitraum hinausgehen könnte, was insbesondere bei Sicherheitsaktualisierungen der Fall sein könnte**. […]

23

Mangelfolgen im Kaufrecht, § 437 Nr. 1-3



24

Produkthaftung i.e.S. gemäß § 1 ProdHG

Voraussetzungen

1. **Rechtsgutsverletzung**: Leben, Körper, Gesundheit, Sache nur bei Privatgebrauch (nicht: fehlerhaftes Produkt selbst)
2. **Fehler** eines **Produkts** (§§ 2, 3)
3. **Kausalität** des Produktfehlers für die Rechtsgutsverletzung
4. **Anspruchsgegner**: Hersteller, Quasi-Hersteller, Importeur, ggf. auch Lieferant (§ 4)
5. Kein Ausschluss nach § 1, insbesondere **Entwicklungsrisiko** (§ 1 II Nr. 5)

Rechtsfolge

- Schadensersatz gemäß §§ 7 ff.
- Kausalität und Zurechnung des Schadens
- Mitverschulden, § 6 ProdHaftG, § 254 BGB
- §§ 9, 7: Rente und Ansprüche Dritter
- §§ 10, 11: Höchstbetrag, Selbstbeteiligung

25

Produkthaftung gemäß ProdHaftG

§ 2 Produkt

Produkt im Sinne dieses Gesetzes ist jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet, sowie Elektrizität.

26

Prof. Dr. Ruth Janal, LL.M.

Entwicklungsrisiko

Definition

- Risiko, das im Zeitpunkt des Inverkehrbringens bereits von dem Produkt ausgeht, zu diesem Zeitpunkt aber nach dem Stand von Wissenschaft und Technik noch nicht erkennbar ist

Haftung

- Keine Verkehrssicherungspflicht gegen Entwicklungsrisiken im Rahmen des § 823 I
- Ausschluss der Haftung für Entwicklungsrisiken nach § 1 II Nr. 5 ProdHaftG
- Haftung bei Arzneimitteln nach § 84 I Nr. 1 Arzneimittelgesetz

27

Prof. Dr. Ruth Janal, LL.M.

Produzentenhaftung gemäß § 823 Abs. 1 BGB

Voraussetzungen

1. **Verletzung** eines der genannten **Rechtsgüter** (NICHT: Vermögen, fehlerhaftes Produkt selbst)
2. Verletzung einer **Verkehrssicherungspflicht** (durch positives Tun oder Unterlassen)
3. **Kausalität** und Zurechnung des Verhaltens für die Rechtsgutsverletzung
4. Keine Rechtfertigungsgründe
5. **Verschulden**: Vorsatz oder Fahrlässigkeit, siehe § 276
6. Kausaler **Schaden**

Rechtsfolge

- Schadensersatz gemäß §§ 249 ff.
- Kausalität und Zurechnung des Schadens
- Mitverschulden, § 254
- §§ 843, 844: Rente und Ansprüche Dritter

28

Prof. Dr. Ruth Janal, LL.M.

Produktbeobachtungspflicht

Beobachtungspflicht

- Pflicht zur aktiven Beobachtung potentieller Schadensrisiken bzgl. der eigenen Produkte, Konkurrenzprodukte und typischer Zubehör- und Kombinationsprodukte
- passive Pflicht zur Entgegennahme von Beschwerden

Reaktionspflicht

- Produktumstellung
- Gefahrenwarnung an Nutzer
- ggf. Rückruf

Zumutbarkeit

- Inhalt und Umfang der Instruktion bestimmen sich nach dem Umfang der Gefahr und der Wahrscheinlichkeit eines Schadenseintritts

29

Prof. Dr. Ruth Janal, LL.M.

Herausforderung Cybersecurity

I. Fehlende Körperlichkeit

- ProdSG und ProdHaftG knüpfen an den Produktbegriff (= bewegliche Sache) an
- Software ist (sofern keine embedded Software) kein Produkt (str.)

II. Klassische Schutzgüter

- ProdSG schützt nur die Sicherheit und Gesundheit von Personen
- ProdHaftG schützt neben Körper und Leben nur das Eigentum an Sachen zum Privatgebrauch
- § 823 I BGB schützt nicht das Vermögen als solches
- **ergo:** Beeinträchtigungen von Sachen, Vermögen, Persönlichkeitsrechten sind teils nicht erfasst

III. Dynamik

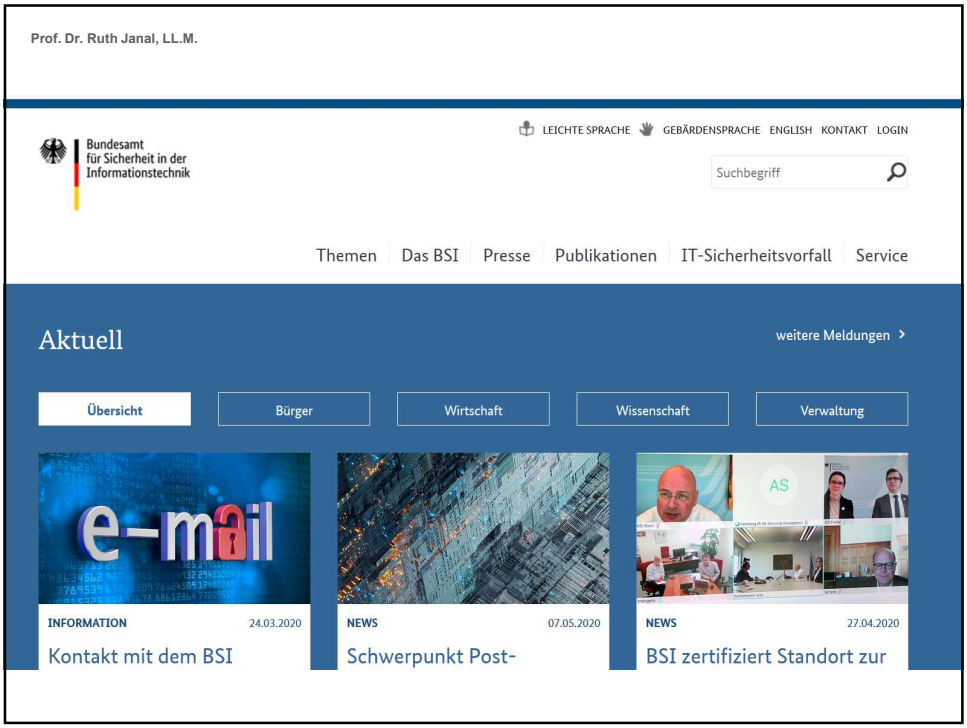
- Zertifizierungen stellen auf den Zeitpunkt des Inverkehrbringens ab; Software bedarf allerdings ständiger Updates zur Gewährleistung der Kompatibilität und Sicherheit

30

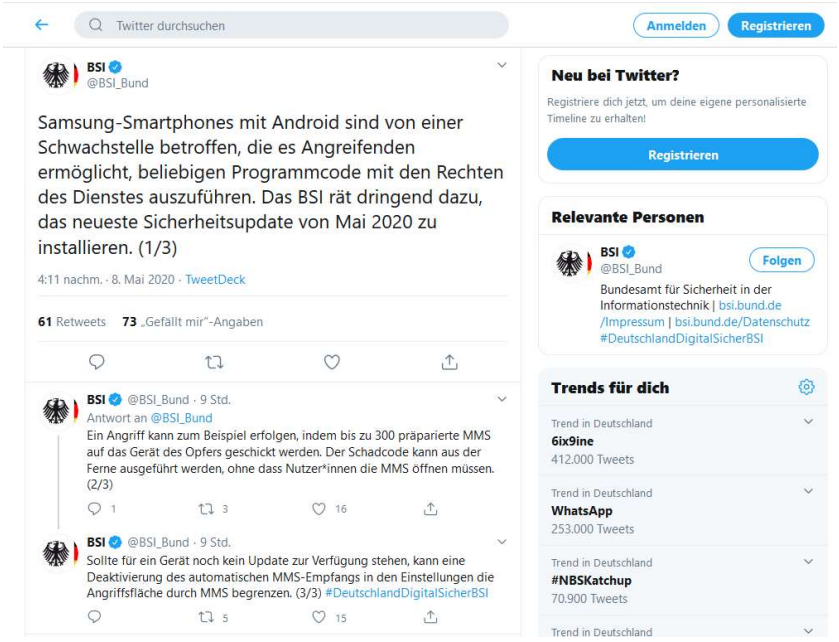
Vorlesung Technikrecht
Cybersecurity: Das BSI-Gesetz

Prof. Dr. Ruth Janal, LL.M.

31



32



33

Kritische Infrastrukturen, § 2 Abs. 10 BSIG

Einrichtungen und Anlagen (oder Teile davon)

Sektoren:

Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen

hohe Bedeutung für das Gemeinwesen:

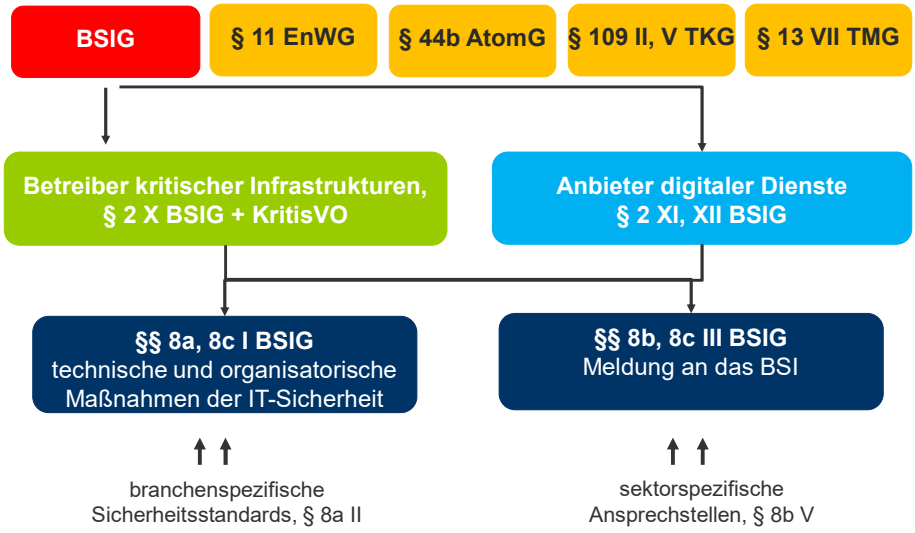
erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit im Falle des Ausfalls oder der Beeinträchtigung

→ **näher bestimmt durch KritisVO nach § 10 I BSIG**

34

Prof. Dr. Ruth Janal, LL.M.

BSI-Gesetz: Maßnahmen



35

Prof. Dr. Ruth Janal, LL.M.

Referentenentwurf zur Reform des BSI-Gesetzes (29.3.2019)

Stärkung der Rolle des BSI

- zunehmend Aufgaben des Verbraucherschutzes, z.B. IT-Sicherheitskennzeichen

Ausweitung des Anwendungsbereichs

- Kritis auch: Abfallentsorgung, Kultur & Medien, Chemie & Automobilsektor
- Hersteller von KRITIS-Komponenten müssen die Vertrauenswürdigkeit ihrer gesamte Lieferkette sicherstellen

Deutlich höhere Bußgelder

36

Vorlesung Technikrecht
Cybersecurity: DSGVO und Cybersecurity Act

Prof. Dr. Ruth Janal, LL.M.

37

Art. 1 DSGVO

Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

[…]

38

Art. 25 DSGVO

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (= Privacy by Design and by Default)

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und […] **trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen** — wie z. B. Pseudonymisierung, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen […].

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. […] Solche Maßnahmen müssen insbesondere **sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden**.

[…]

39

Datenschutz-Grundverordnung (DSGVO)

Art. 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

[…]

40

Cybersecurity Act, VO (EU) 2019/881

ENISA

- Agentur der Europäischen Union für Cybersicherheit
- Ausarbeitung der Zertifizierungssysteme
- Cybersicherheitsübungen
- unionsweiter Informationsaustausch

Europäischer Zertifizierungsrahmen

- EU-weit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit
- grds. Freiwilligkeit, es sei denn, anderweitige Regelung
- Festlegung von drei Vertrauensgraden: niedrig, mittel und hoch

41

Art. 52 CA

Vertrauensgrad „mittel“:

- Geringhaltung bekannter Cybersicherheitsrisiken und Attacken von Akteuren mit begrenzten Fähigkeiten und Ressourcen
- externe Zertifizierung

Problem: Marktüberwachung nicht adressiert!

Vertrauensgrad „niedrig“:

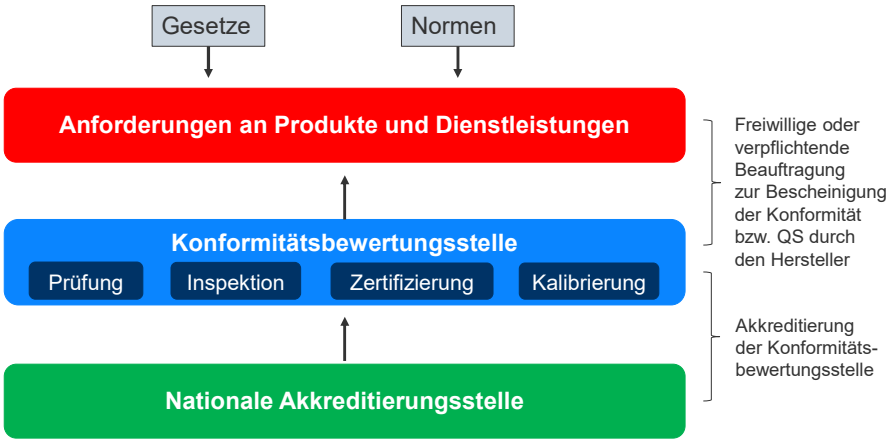
- Geringhaltung der bekannten grundlegenden Risiken
- grds. externe Zertifizierung, aber auch Eigenbewertung möglich.

Vertrauensgrad „hoch“:

- neuester Stand der Technik
- Geringhaltung von Attacken durch Akteure mit umfangreichen Fähigkeiten und Ressourcen
- Zertifikat soll grds. von einer Behörde erteilt werden

42

Mess- und Prüfwesen



43

Cybersecurity Act: Kritik

I. Nicht geregelte Marktüberwachung

II. Keine Mindeststandards

- Produkt enthält keine bekannten und ausnutzbaren Sicherheitslücken
- Produkt ist sicher updatebar
- Hersteller informiert Behörden über Sicherheitslücken

III. Existenz etablierter internationaler Zertifizierungssysteme

44

45

Probleme mit Zertifikaten

1. Komplexität von Software / fehlende Nachvollziehbarkeit
2. Mangel an ausreichendem Fachpersonal
3. Dauer / Aufwand der Zertifizierung
4. IT-Sicherheit ist kein Zustand, sondern ein Prozess!

46