

# Update Datenschutzrecht, Recht der Netz- und Informationssicherheit

**Secure Linux Administration Conference, Berlin**

**Michael Stolze, LL.M. LL.M.**

Rechtsanwalt, externer betrieblicher Datenschutzbeauftragter

TÜV geprüfter Datenschutzbeauftragter + Datenschutzauditor

Master of Laws – IT-Recht & Recht des Geistigen Eigentums (Universität Hannover)

Master of Laws – Information and Communication Technology Law (Universität Oslo)

# Agenda

- Update IT-Recht
- Schwerpunkt IT-Sicherheit
  - Aktuelle Einordnung
  - Mehr Transparenz und Kontrolle in der IT
  - Workshop: Vereinzelte Fragen zum Mindeststandard ISMS

Update: IT Recht

# Verfassungsbeschwerden gegen die Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung teilweise erfolgreich

Pressemitteilung Nr. 19/2016 vom 20. April 2016

Urteil vom 20. April 2016

1 BvR 966/09, 1 BvR 1140/09

„Verdeckte Eingriffe in informationstechnische Systeme“  
(Staatstrojaner)

Status: Freies WLAN und die Störerhaftung

# Status: Freies WLAN und die Störerhaftung

31. Mai 2016, 17:31 Uhr Störerhaftung

## Abmahnanwälte stöhnen - Internetnutzer jubeln

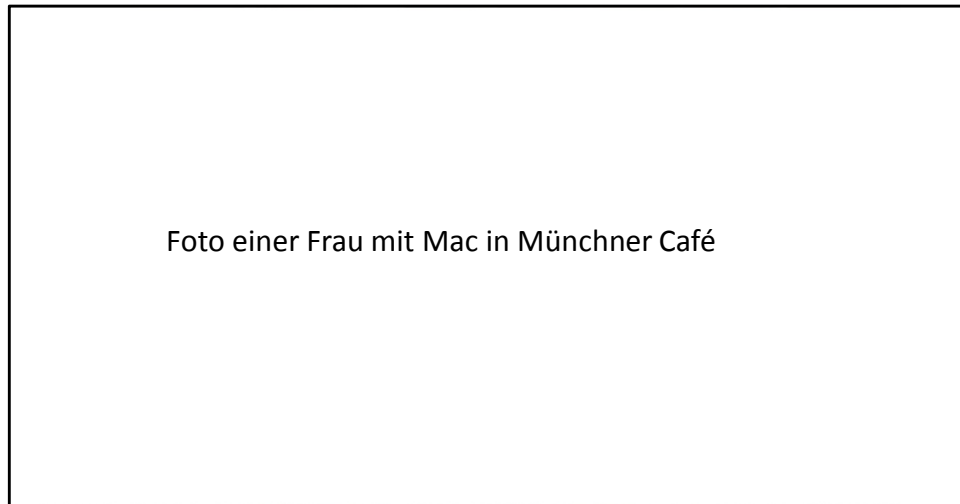


Foto einer Frau mit Mac in Münchner Café

Mal schnell ins Netz? In Münchner Cafés ist das kein Problem. (Foto: Robert Schlesinger/dpa)

- Die Koalition schafft die Wlan-Störerhaftung ab.
- Das hieß es bereits Anfang Mai, damals war jedoch unklar, wie weitreichend die neue Regelung tatsächlich ausfällt.
- In der Gesetzesbegründung wird deutlich, dass die Regierung Wlan-Anbieter vor der Übernahme von Abmahn- und Gerichtskosten schützen will.

Von *Guido Bohsem, Berlin*

Quelle: <http://www.sueddeutsche.de/digital/stoererhaftung-abmahnnaewelte-stoehnen-internetnutzer-jubeln-1.3013287>

## Status: Freies WLAN und die Störerhaftung

- Es war einmal vor langer Zeit eine glasklare Regelung...
- **Art. 12 Abs. 1 InfoSocRL (2000/31/EG) - Reine Durchleitung**  
Die Mitgliedstaaten stellen sicher, dass [ein Access Provider] **nicht** für die übermittelten Informationen **verantwortlich** ist, sofern er
  - a) die Übermittlung **nicht** veranlasst,
  - b) den Adressaten der übermittelten Informationen **nicht** auswählt und
  - c) die übermittelten Informationen **nicht** auswählt oder verändert.

# Status: Freies WLAN und die Störerhaftung

- **§ 8 Abs. 1 TMG**

Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, **nicht** verantwortlich, sofern sie

1. die Übermittlung **nicht** veranlasst,
2. den Adressaten der übermittelten Informationen **nicht** ausgewählt und
3. die übermittelten Informationen **nicht** ausgewählt oder verändert haben.

- **Neuer Absatz 3**

Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.



# Status: Freies WLAN und die Störerhaftung

- Begründung zum Änderungsantrag:  
„Die Haftungsprivilegierung des Diensteanbieters nach § 8 Absatz 1 und 2 umfasst z.B. uneingeschränkt auch die verschuldensunabhängige Haftung im Zivilrecht nach der sog. Störerhaftung und steht daher nicht nur einer Verurteilung des Vermittlers zur Zahlung von Schadenersatz, sondern auch seiner Verurteilung zur Tragung der Abmahnkosten und der gerichtlichen Kosten im Zusammenhang mit der von einem Dritten durch die Übermittlung von Informationen begangenen Rechtsverletzung entgegen.“ (Begründung zum Änderungsantrag der Fraktionen der CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung-Dr.18/6745, Ausschussdrucksache 18(9)822 vom 31.05.2016).
- „Denn die Auslegung ist vorrangig an dem objektiven Sinn und Zweck des Gesetzes zu orientieren und kann durch Motive, die im Gesetzgebungsverfahren dargelegt wurden, im Gesetzeswortlaut aber keinen Ausdruck gefunden haben, nicht gebunden werden“ – BGH, KVR 4/94

Konsequenzen?

# Status: Freies WLAN und die Störerhaftung



A screenshot of a Twitter post. The user is Joerg Heidrich (@dasgesetzbinich), dated 5. Juni. The text of the tweet reads: 'Unfassbar überrschende Entwicklung: Abmahnindustrie für WLAN läuft weiter. #Stoererhaftung'. Below the text is a large white rectangular area with the text 'Foto Hotspot' centered inside. At the bottom of the tweet, there is a link to an article titled 'Anwälte wollen weiter wegen WLAN abmahnen' from m.welt.de, with a brief description: 'Die Bundesregierung wollte die Anbieter von drahtlosen Internet-Zugängen eigentlich aus jeglicher Haftung für illegale Up- oder Downloads entlassen...'. The tweet shows 103 retweets and 50 likes.

Joerg Heidrich @dasgesetzbinich · 5. Juni

Unfassbar überrschende Entwicklung:  
Abmahnindustrie für WLAN läuft weiter.  
**#Stoererhaftung**

Foto Hotspot

**Anwälte wollen weiter wegen WLAN abmahnen**  
Die Bundesregierung wollte die Anbieter von drahtlosen Internet-Zugängen eigentlich aus jeglicher Haftung für illegale Up- oder Downloads entlassen...  
m.welt.de

103 50

# Status: Freies WLAN und die Störerhaftung



**Joerg Heidrich**

@dasgesetzbinich

Oh ja! Die gute, alte Vorschaltseite! Wie viele Terroranschläge und Urheberraubmorde die schon verhindert hat!

### **WLAN und Störerhaftung: Die Fronten sind verhärtet**

Die Koalition kommt bei der geplanten Reform des Telemediengesetzes nicht zu Potte. In der Regierung wächst offenbar der Widerstand gegen eine Vorschaltseite für Hotsp...  
[heise.de](http://heise.de)

RETWEETS	GEFÄLLT
7	7

05:50 - 15. Apr. 2016



# Status: Freies WLAN und die Störerhaftung

 **beck-online**  
@beckonlinede

 Folgen

Rechtsausschuss des Bundesrats folgt  
Entschließungsantrag mehrerer Bundesländer  
zur WLAN-Störerhaftung – [ch.beck.de](http://ch.beck.de/1Uj5zFG)  
[/1Uj5zFG](http://ch.beck.de/1Uj5zFG)

RETWEETS

4



01:37 - 15. Juni 2016



# Status: Freies WLAN und die Störerhaftung

 **SPD Parteivorstand**   
@spdde 

Wir beenden die [#Störerhaftung](#) =  
Rechtssicherheit für WLAN-Betreiber + freies  
WLAN! Mehr: [spdlink.de/smBG](http://spdlink.de/smBG)



RETWEETS 44    GEFÄLLT 70



05:09 - 11. Mai 2016

Foto: Eugenio Marongiu/Shutterstock.com

  44     70    

Status: Cookie-Hinweise



Die neue Daimler Global Media Site  
Jetzt live in ne...

**/daimler\_news**  
Sicherheit hat oberste Priorität – auch bei rechtlichen Fragen.:  
Automatisiertes und autonomes Fahren hat gro... <https://t.co/g17sPDBa5q>  
16.06.2016 @daimler\_news

**/Joerg\_Howe**  
RT @mbfussball: Unterstütze jetzt das DFB-Team und zeig deinen Support im

### Verwendung von Cookies

Um die Webseite optimal gestalten und fortlaufend verbessern zu können, verwendet Daimler Cookies. Durch die weitere Nutzung der Webseite stimmen Sie der Verwendung von Cookies zu.

[Weitere Informationen erhalten Sie in den Cookie-Hinweisen >](#) [Schließen >](#)

Daimler-Aktie  
€ **55,31** ↓ -0,36%  
Kurs mindestens 15 Min. zeitverzögert.  
16.06.2016 / 17:35

Services  
[> Kontakt](#)  
[> Download Berichte & Broschüren](#)





# Update: IT Recht

## **Wirksame Einwilligung in die Nutzung von Cookies**

- Einwilligung durch vorformulierte Einwilligungserklärung zulässig, wenn der Nutzer das voreingestellte Häkchen wieder entfernen kann (OLG Frankfurt a.M., Urteil vom 10.12.2015 – Az. 2-6 O 30/14).

# Update: IT Recht

## **Außerordentliche Kündigung wegen Erschleichen von Administratorenrechten**

- Erweiterung der eigenen Zugriffsberechtigung auf vollständige Lese- und Schreibrechte am Qualitätssicherungssystem.
- Erweckter Eindruck, Manipulation durch Arbeitskollegen
- Verschaffung Zugriffsrechte nach „Art eines Hackers“
- LAG München: Urteil vom 05.08.2009 – 11 Sa 1066/08

# Update: IT Recht

## **„Fotoklau“ bei „lizenzfreien“ Bildern**

- Lizenzeinräumung bedingt durch Urheberbenennung.
- KG Berlin, Beschluss vom 26.10.2015, Az. 24 U 111/15 (Pixelio):  
„Bedingung“ in AGB rechtstechnisch nicht ausreichend.
- Schadensersatz 100,00 EUR ohne Verletzerzuschlag
- Überhaupt Unterlassungsanspruch?
- Gilt auch für flickr?

# Update: IT Recht

## **Abmahngefahr Datenschutzerklärung auf Websites**

- Fehlende Datenschutzerklärung auf Webseite ist ein Wettbewerbsverstoß (OLG Köln, Urteil vom 11.03.2016 – Az. 6 U 121/15).

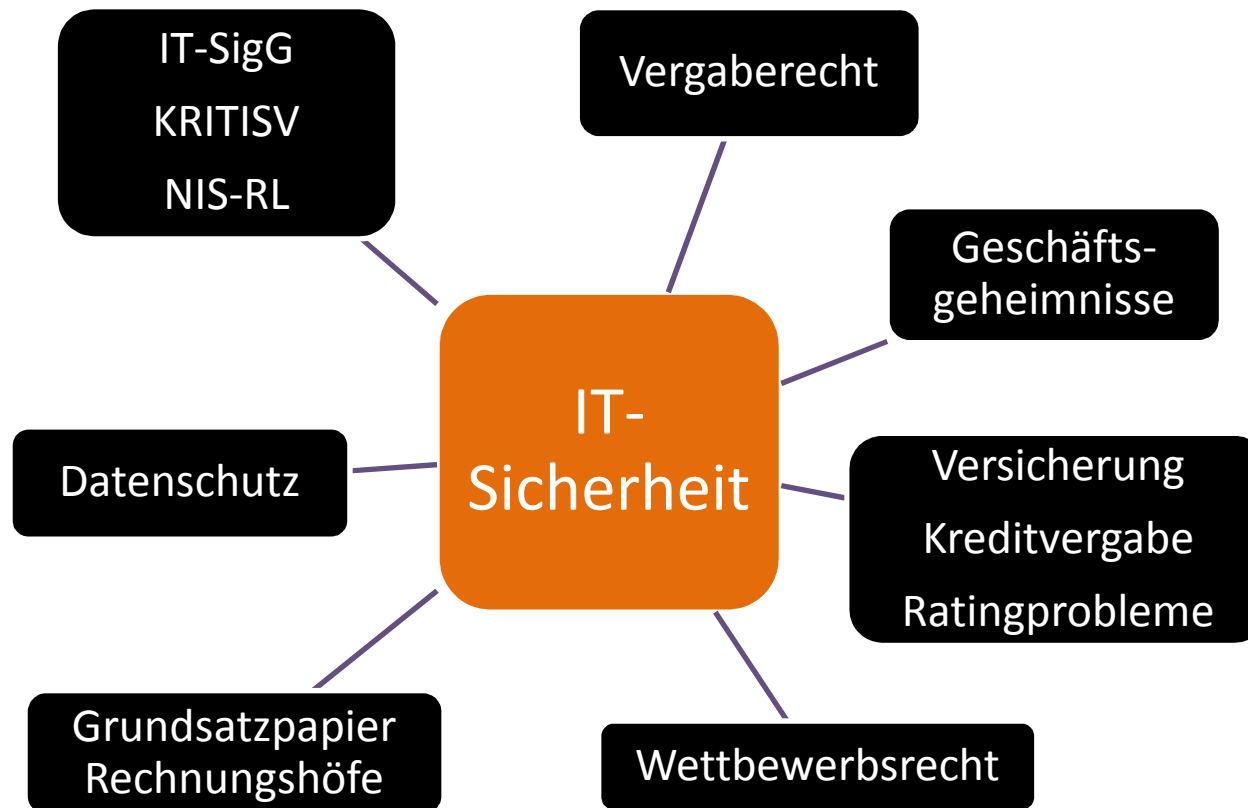
# Update: IT Recht

## **Open Source**

- LG Bochum, Urteil vom 03.03.2016 – Az. I – 8 0 294/15: Fehlende Beilage von Quellcode und Lizenzbedingungen begründet Schadensersatzanspruch.
- Kostenlose Nutzungsmöglichkeit unter dem Vorbehalt der Lizenzbedingungen steht Schadensersatz und Streitwert über 1.000,000,00 EUR nicht entgegen.

**15 Minuten Pause**

IT-Sicherheit





# IT-Sicherheit – Kernbereichsaufgabe

# Aktuelle Entwicklungen

- IT-SiG 2015
- KRITISV 2016
- NIS-Richtlinie 2015
- DSGVO
- Grundsatzpapier Rechnungshöfe 2015

# Aktuelle Entwicklungen

- Was bedeutet das alles für IT-Verantwortliche?
  - Mehr Reglementierung
  - Mehr Budget (wahrscheinlich, zumindest hoffentlich)
  - Mehr Transparenz
  - Mehr Kontrolle (Art. 39 Abs. 1 b DSGVO – Überwachung durch bDSB)

# IT-Sicherheit – Kernbereichsaufgabe

# IT-Sicherheit – Kernbereichsaufgabe

???

## Exkurs Kernbereichsaufgabe

- § 76 Abs. 1 AktG

Der Vorstand hat unter eigener Verantwortung die Gesellschaft zu leiten.

- §§ 116, 93 AktG

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein **Überwachungssystem** einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

# Handlungspflichten

- § 93 Abs. 2 S.1 AktG

Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als **Gesamtschuldner** verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.

- §§ 116, 93 AktG

Für die Sorgfaltspflicht und Verantwortlichkeit der Aufsichtsratsmitglieder gilt § 93 [...] sinngemäß.

# Normadressaten und Sorgfaltsmaßstäbe

- § 43 GmbHG
  - (1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
  - (2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft **solidarisch** für den entstandenen Schaden.
- § 91 Abs. 2 AktG analog (vgl. auch amt. Begr. KonTraG)

Die [Geschäftsführung] hat geeignete Maßnahmen zu treffen, insbesondere ein **Überwachungssystem** einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.



Pflicht: Einführung Überwachungssystem

## Mögliche Rechtsfolgen bei Verstößen

# Mögliche Rechtsfolgen bei Verstößen

- Schadensersatz aus Vertrag § 280 BGB (Pflichtverletzung)
- Mitverschulden nach § 254 BGB, z.B. bei Mitwirkungspflichten
- Schadensersatz nach § 823 BGB (Organisationsverschulden)
- Schadensersatz nach §§ 7, 8 BDSG
- Abmahnung wegen unlauterem Handeln, z.B. § 7 UWG (SPAM)
- Informations- bzw. Meldepflichten, § 42a BDSG, § 109a TKG, § 15a TMG, § 44b AtG, § 11 EnWG, § 8n BSIG
- Verlust des Versicherungsschutzes
- Probleme bei der Finanzierung
- Strafrecht / Bußgeld (§ 130 Abs. 1 i.V.m. § 30 OWiG)
- Negativer Prüfungsvermerk im Jahresabschluss (AG, GmbH, GmbH & Co.KG)

# IT-Sicherheit – Anforderungen an die KRITIS

# Anforderungen für die KRITIS

- **§ 8a Abs. 1 BSIG**

Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

# Anforderungen für die KRITIS

- **§ 8a Abs. 1 BSIG**

Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. **Dabei soll der Stand der Technik eingehalten werden.** Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

# Anforderungen für die KRITIS

- **§ 8a Abs. 1 BSIG**

Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

## ISO 27001 Stand der Technik?

- Branchenspezifische Regelung des IT-Sicherheitskatalogs gemäß § 11 Abs. 1a Energiewirtschaftsgesetz mit der Kernforderung der Einführung eines ISMS gemäß DIN 27001
- Maßstab für die gesamte KRITIS?



# Meldepflichten für die KRITIS

- **§ 8a Abs. 3 BSIG**

Die [KRITIS] haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen [...].

Das [BSI] kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und

2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.

# Meldepflichten für die KRITIS

- **§ 8b Abs. 3 BSIG – Eingehende Meldungen**

Die [KRITIS] haben dem [BSI] binnen sechs Monaten nach Inkrafttreten der [KRITISV] eine **Kontaktstelle** für die Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu benennen. **Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind.** Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

# Meldepflichten für die KRITIS

- **§ 8b Abs. 4 BSIG – Ausgehende Meldungen**

[Die KRITIS hat] erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1.führen können oder

2.geführt haben,

über die Kontaktstelle unverzüglich an das [BSI] zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

# Meldepflichten für die KRITIS

- **§ 8b Abs. 4 BSIG – Ausgehende Meldungen**

[Die KRITIS hat] erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

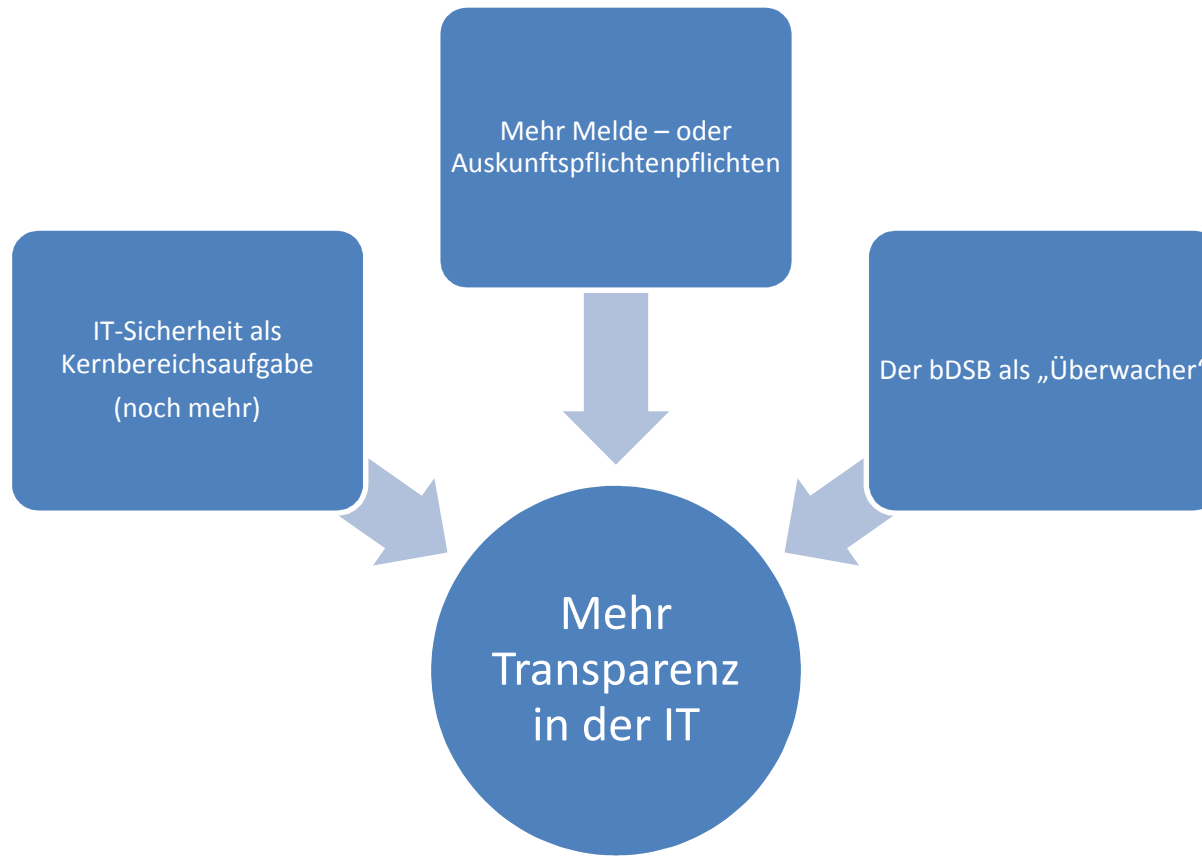
1.führen können oder

2.geführt haben,

über die Kontaktstelle unverzüglich an das [BSI] zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

# IT-Sicherheit – Meldepflichten und Transparenz im Fokus

# IT-Sicherheit – Meldepflichten und Transparenz



**Haben Sie noch Fragen?**

**Vielen Dank für die Aufmerksamkeit!**

**Michael Stolze, LL.M. LL.M.**

Rechtsanwalt, externer betrieblicher Datenschutzbeauftragter

TÜV geprüfter Datenschutzbeauftragter + Datenschutzauditor

Master of Laws – IT-Recht & Recht des Geistigen Eigentums (Universität Hannover)

Master of Laws – Information and Communication Technology Law (Universität Oslo)

Döhrbruch 62 · 30559 Hannover

Tel 0511 / 473906-0

Fax 0511 / 473906-7

[stolze@recht-freundlich.de](mailto:stolze@recht-freundlich.de)