LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

LMU Rechtsinformatikzentrum

Thomas Hofer, Akademischer Direktor

Das neue IT-Sicherheitsgesetz - was kommt auf den Öffentlichen Sektor zu?

14.10.2015

IT-Sicherheitsgesetz: Neue Pflichten für kommunale Wasserversorger und Abwasserentsorger

Search

WEBCAMS. ROUTERS.

Hessen und Rheinland-Pfalz: Kfz-Zulassungsstellen müssen nach Hackerattacke Arbeit einstellen

TAKE A TOUR FREE SIGN UP

„Cyber-Angriffe finden täglich statt und werden zunehmend professioneller und zielgerichteter ausgeführt."

HACKERANGRIFF

Digitale Sorglosigkeit ist für alle Firmen gefährlich

DEVELOPER API

Dienstag, 14. April 2015

"Keine Science Fiction mehr"

Täglich Cyberangriffe auf Bundesregierung

Gehackte Bundestags-Rechner

Cyber-Angriff kam per E-Mail

IN THE PRESS

IT und Netzpolitik | IT- und Cybersicherheit | Pressemitteilung 12.06.2015

Bundestag verabschiedet IT-Sicherheitsgesetz

Bundesinnenminister de Maizière: "Wichtiger Schritt zur Stärkung der IT-Systeme in unserem Land"

It's a reminder to many to know what's on your network...

darkREADING

Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan.

AARGAUER ZEITUNG

51 Milliarden Euro Schaden pro Jahr

Bitte schätzen Sie den Schaden Ihres Unternehmens in Deutschland innerhalb der letzten 2 Jahre durch den jeweiligen aufgetretenen Delikttyp ein?

Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	23,0 Mrd.
Patentrechtsverletzungen (auch vor der Anmeldung)	18,8 Mrd.
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	14,3 Mrd.
Ausfall, Diebstahl oder Schädigung von IT-Systemen, Produktions- oder Betriebsabläufen	13,0 Mrd.
Imageschaden bei Kunden oder Lieferanten / Negative Medienberichterstattung	12,8 Mrd.
Kosten für Rechtsstreitigkeiten	11,8 Mrd.
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	3,9 Mrd.
Erpressung mit gestohlenen Daten	2,9 Mrd.
Höhere Mitarbeiterfluktuation / Abwerben von Mitarbeitern	1,7 Mrd.
Sonstige Schäden	0,2 Mrd.
Gesamtschaden innerhalb der letzten 2 Jahre	**102,4 Mrd.**

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550)
Quelle: Bitkom Research
8

BITKOM

Fakten & Zahlen

Agenda

- IT-Sicherheit und Compliance
- Zielsetzungen des IT-Sicherheitsgesetzes (IT-SiG)
- „Konstruktion“ IT-SiG
- Kernregelungen
- Bedeutung für Öffentlichen Sektor
- Umsetzung - Einzelfragen
- Fazit und Ausblick

Allgemeiner Haftungsmaßstab

§ 276 Abs. 2 BGB:

„Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt.“

- Reduzierung des Risikos von Schadensereignissen
- Beachtung der jeweils geforderten Sorgfalt

Bundesgerichtshofes (BGH) spricht im Rahmen der Haftungssystematik von **Verkehrssicherungspflichten**:

„Wer eine Gefahrenquelle eröffnet oder sich an ihr beteiligt, muss Dritte schützen und hierfür geeignete Schutzmaßnahmen ergreifen.“

Verkehrssicherungspflichten ergeben sich aus:

- ✓ ***Gesetzlichen Bestimmungen***
- ✓ *Vertraglichen Bestimmungen bzw. einbezogenen Richtlinien*
- ✓ *Vorgaben der Rechtsprechung; DIN-/ISO-Normen; Branchengepflogenheiten*

Compliance-Begriff

*„**Compliance**“* bedeutet grundsätzlich: ***Einhaltung von Vorschriften*** für Unternehmen (Gesetze, Regeln und Richtlinien - rechtlich, ethisch etc.)

= ***Status***, der die Zielerreichung abbildet

und /oder

= ***Prozesse und Maßnahmen***, die Compliance anstreben und sichern (z.B. durch Vergleich Soll-Ist-Zustand; Überwachungsmaßnahmen sowie Sanktionierung.

Übergeordnetes Ziel jeder Compliance:

„Vermeidung rechtswidriger und aus anderweitigen Gründen inakzeptabler Zustände“

„IT-Compliance-Gesetzbuch“?

- **Querschnittsmaterie,** bislang keine einheitliche gesetzliche Regelung
- **Anknüpfungspunkte in verschiedenen Gesetzen** / Normen, insbes.:
  - Grund-/Persönlichkeitsrechte (Art.1; 2 GG; § 12 BGB; § 22f KUrhG)
  - Gewerblicher Rechtsschutz (insbes. Urheber-, Markenrecht)
  - Strafgesetze (StGB und Nebenstrafrecht); OWiG
  - Telekommunikationsgesetz (TKG)
  - Telemediengesetz (TMG)
  - BDSG (→ § 9 BDSG + Anlage)
  - NEU: BSI-G
  - Satzungen, Richtlinien, Betriebsvereinbarungen
  - Arbeitsvertrag; Individualvereinbarungen

… und bei Verstößen kommt die Cyber-Polizei!?

Spannungsfeld..

Öffentliche Verwaltung in Bewertung und Bewältigung häufig überfordert?!

Betrieb

Aufrechterhalten
Effizienz und Ergebnis steigern
gesetzeskonform
Verträge einhalten

Personal

Technik
(Komplexität, Vernetzung, Virtualisierung, Sicherheit)

Organisation
(Automatisierung, Integration, Geschäftsmodell)

Normen & Standards
(Zertifizierungen?)

Kosten

Risiken

Gesetze
(neu: IT-SiG)

Richtlinien

IT-Governance

Angriffe

Schäden

Benutzer

Bequemlichkeit

Know-How

„Trendfolger“

Rechtsvorteile durch Standards

- Ziel:
  Nachweis des Sicherheitsniveaus (Verkehrssicherungspflichten) durch anerkannte Audits und Zertifizierung(en)
- Anforderung:
  Ein Standard muss so detailliert sein, dass er das konkrete Problem im Schadensfall ausreichend abbildet.
- Beweislastverteilung im IT-Umfeld:
  Wenn Standard eingehalten, hat der Geschädigte zu beweisen, welche Maßnahme(n) darüber hinaus konkret erforderlich, geeignet und zur Schadensvermeidung im konkreten Fall dem IT-Betreiber zumutbar war(en).
- Unterstützt gerichtliche Sachverständigengutachten
- Kosten-/Nutzenrelation individuell zu bestimmen

Rechtliche Anknüpfungspunkte

„Initiativen“ zur Regelung / Standardisierung von IT-Sicherheit:

- Standards und Best Practices: BSI IT-Grundschutz-Kataloge (14. EL); Leitfäden, Goldene Regeln etc.
- ISO 27001, 27002, 27018 - ISO/IEC 38500 - CobiT – ITIL
- ISIS12; ISA+
- IDW Prüfungsstandards
- Brancheninitiativen: z.B. Eco, BITKOM-Leitfäden und Positionspapiere

Ausgangslage IT-SiG

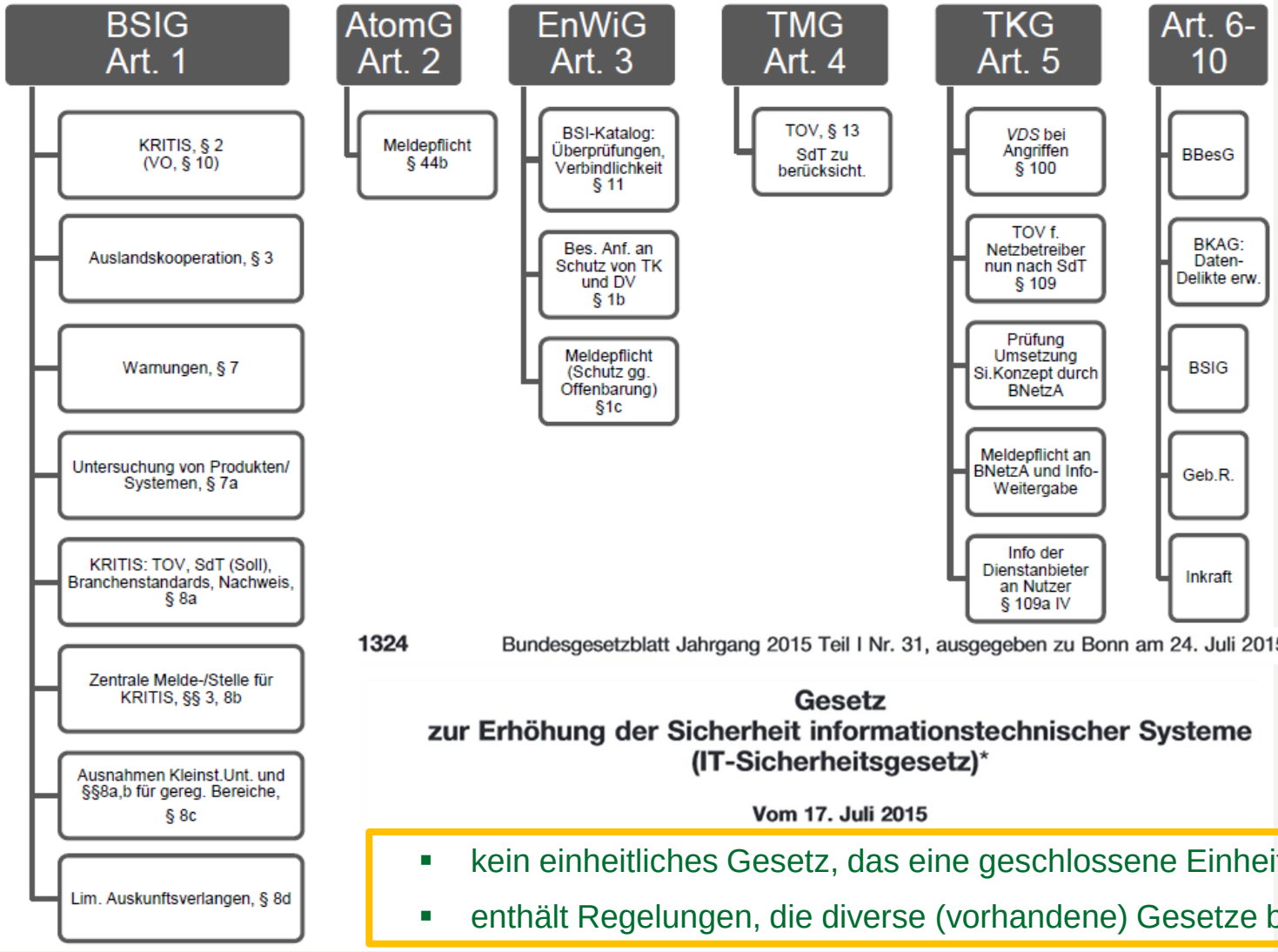
- Verbesserung des Schutzes der Verfügbarkeit, Integrität und Vertraulichkeit datenverarbeitender Systeme (so bereits BVerfG 2008)
- **Anpassung an veränderte Bedrohungslage**
  Cybersicherheit zentraler Baustein der Inneren Sicherheit
  (→ Informationssicherheit in der öffentlichen Wahrnehmung bisweilen im Schatten des Datenschutzes)

Ziele IT-SiG

Im Einzelnen:

1. *Schutz der Funktionsfähigkeit des Staates / krit. Infrastruktur*
2. *"verbessertes Bild zur IT-Sicherheitslage" in Deutschland gewinnen (→ Detektion vorrangiges Interesse des BSI)*
3. *Schutz der Unternehmen vor Spionage und Ausspähung*
4. *Verstärkter Schutz der Bürgerinnen und Bürger in sicherem Netz*
5. *Ausbau der IT–Sicherheit in der Bundesverwaltung*

Konstruktion IT-Sicherheitsgesetz



- kein einheitliches Gesetz, das eine geschlossene Einheit darstellt
- enthält Regelungen, die diverse (vorhandene) Gesetze betreffen

Wer ist „kritischer Infrastrukturanbieter“?

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
§ 10 Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.
(2) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.

- Betriebe, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind,
- Sektorenzugehörigkeit: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen
- Fehlerfolgenerheblichkeit: Hohe Bedeutung für Funktionieren des Gemeinwesens (=Qualität), weil durch Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (=Quantität)

Kritische Dienstleistungen im Rahmen der Sektoren nach Gesetzesbegründung zu § 2 Abs. 10 Nr. 1 BSI-Gesetz (I):

- **Sektor Energie**
  - ✓ Stromversorgung
  - ✓ Versorgung mit Erdgas
  - ✓ Versorgung mit Mineralöl
- **Sektor der Informationstechnik und Telekommunikation**
  - ✓ Sprach- und Datenkommunikation
  - ✓ Verarbeitung und Speicherung von Daten
- **Sektor Transport und Verkehr**
  - ✓ Transport von Gütern
  - ✓ Transport von Personen im Nahbereich
  - ✓ Transport von Personen im Fernbereich
- **Sektor Wasser**
  - ✓ Trinkwasserversorgung
  - ✓ Abwasserbeseitigung

Kritische Dienstleistungen im Rahmen der Sektoren nach Gesetzesbegründung zu § 2 Abs. 10 Nr. 1 BSI-Gesetz (II):

- **Sektor Gesundheit**
  - ✓ Medizinische Versorgung
  - ✓ Versorgung mit Arzneimitteln und Medizinprodukten
- **Sektor Ernährung**
  - ✓ Versorgung mit Lebensmitteln
- **Sektor Finanz- und Versicherungswesen**
  - ✓ Zahlungsverkehr, Zahlungsdienstleistung durch Überweisung, Zahlungskarten und E-Geld
  - ✓ Bargeldversorgung
  - ✓ Kreditvergabe??
  - ✓ Geld- und Devisenhandel?
  - ✓ Wertpapier- und Derivathandel??
  - ✓ Versicherungsleistungen?

WEN betrifft das IT-SiG mit Inkrafttreten der RechtsVO gem. § 10 BSI-G?

- § § 2 Abs. 10, 10 Abs. 1 BSIG Rechtsverordnung (Entwurf des BMI bis Ende 2015, Diskussion mit der Öffentlichkeit in Q 1 2016):
  konkretisiert IT-SiG und legt kritische Schwellenwerte fest, ab wann ein Unternehmen kritische Dienstleistung bereitstellt.
- BSI: ca. 500-1000 Unternehmen betroffen (←Gesetzesbegründung: ca. 2.000 Unternehmen, davon wären allein 416 Sparkassen in Dtld.),
  anstelle konkreter Benennung mess- und handhabbare Kriterien wie beispielsweise Marktanteil an Versorgung einer bestimmten Region mit bestimmter Leistung.
- Sektorale Festlegung, Vorläufer: UP KRITIS des BMI
  → heute 1400 Unternehmen / Einrichtungen

… und wen nicht?

- § 8c I BSIG: Kleinstunternehmen (< 10 Mitarbeiter bzw. < 2 Mio. Jahresumsatz)
- Branchen, die bereits ähnliche oder sogar weitergehende Standards einzuhalten haben, etwa Energieversorger

Wer ist „kritischer Infrastrukturanbieter“ -?

Was meinen Sie zu…

- Flughafen Nürnberg?
- Städtisches Klinikum Nürnberg?
- Kreiskrankenhaus Hersbruck?
- Städtische Werke Lauf a.d.Pegnitz?
- Landratsamt – Straßenverkehrsamt – Weilheim-Schongau?
- Kreissparkasse Würzburg?
- Münchner Verkehrsverbund MVV?
- 1&1?

Kritik…

- IT-SiG verletzt Bestimmtheitsgebot des GG
- IT-SiG berührt mit der Organisationshoheit den Kernbereich der kommunalen Selbstverwaltungsgarantie (Art. 28 Abs. 2 GG):
  - öffentlich-rechtliche Wasserversorgung als Teil der Daseinsvorsorge ein Lehrbuchfall der Leistungsverwaltung und damit der Verwaltung der Kommune zuzuordnen
  - Str., ob Bund gestützt auf die Gesetzgebungskompetenz aus Art. 74 Abs. 1 Ziff. 11 GG Regelungen treffen kann, die die Organisationshoheit der Gemeinden einschränken.
  - Gesetzesbegründung erstreckt IT-SiG nicht auf Verwaltungen der Kommunen, da Bund Gesetzgebungskompetenz fehlt (vgl. BT-Drs. 18/4096, S. 24).
- Konkretisierung unklar: Welche Dienstleistungen gehören genau hierzu?
- Die RVO bleibt abzuwarten; bis zur Verabschiedung Grauzone hinsichtlich der konkret betroffenen Unternehmen.

TOV - § 8a Abs. 1 S. 1 BSIG

Was sind „Technische und Organisatorische Vorkehrungen“ zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit?

- *technisch*: Zugriffskontrolle, Weitergabekontrolle, Updates, Patches…
- organisatorisch: ITSM, Rechtsberatung, IT-Sicherheitsbeauftragter, …
- Schaffung sektor- und branchenspezifische Standards
  - unter Einbeziehung aller betroffenen Kreise (Verwaltung – Wirtschaft – Wissenschaft)
  - Bestimmung in gemeinsamen Arbeitsprozess mit Vertretern der Betreiber und externen Fachleuten

WEN betrifft das Gesetz bereits heute?

Telemediengesetz (TMG): § 13 Pflichten des Diensteanbieters

(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese

a) gegen Verletzungen des Schutzes personenbezogener Daten und

b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

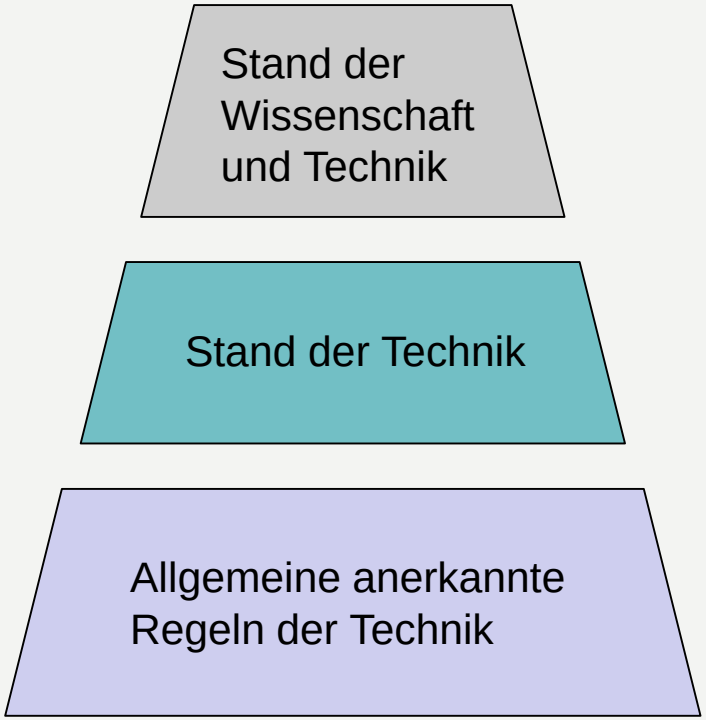
WEN betrifft das Gesetz bereits heute?

- **Informationsanbieter**
  - Konkret: Unternehmens- und Behörden-Websites, Online-Shops, Blogs
  - Gewerbliche Betreiber: auch Behörden, ebenso Privatpersonen und Vereine, wenn mit Webangebot dauerhaft Einnahmen generiert werden sollen (z.B. bezahlte Werbung in Form von Bannern).
  - Stand der Technik ist zu „berücksichtigen“: d.h. verhindern, dass Daten manipuliert oder gestohlen werden (Verschlüsselung), jedoch auch, dass Computerviren oder Trojaner den Rechner des Nutzers infizieren (Viren- und Hacker-Schutz).
  - Keine Kleinstunternehmerausnahme (i.S.v. § 8c I BSIG)
  - Verstöße bußgeldbewehrt (§ 16 TMG)
- **Strom- und Gasnetzbetreiber:** müssen Bundesnetzagentur Ansprechpartner für die IT-Sicherheit bis 30.11.2015 benennen.
- **Bis 31.01.2018**: Alle KRITIS-Unternehmen der Energiebranche (Elektrizität, Gas) müssen ein Informationssicherheits-Managementsystem eingeführt und die Zertifizierung dafür erhalten haben (vgl. IT-Sicherheitskatalog BNetzAgentur)

WAS gilt mit Inkrafttreten der RechtsVO (§ 10 BSI-G)?

- (Nach der VO betroffene) **Betreiber Kritischer Infrastrukturen** werden verpflichtet,
  - die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach *dem Stand der Technik angemessen* abzusichern und –
  - sofern nicht andere Spezialregelungen bestehen – diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen.
  - Nachweis durch Audits, Zertifikate mgl.
  - *erhebliche IT-Sicherheitsvorfälle* dem BSI zu melden (§ 8b Abs.4 BSIG).
  - Voraussetzung dafür: Einrichtung und Aufrechterhalten einer Kontakt- und Meldestelle (24h / 365 T.)
- Ziel: beim BSI zusammenlaufende Informationen über IT-Angriffe auszuwerten und den Betreibern Kritischer Infrastrukturen zur Verbesserung des Schutzes ihrer Infrastrukturen schnellstmöglich zur Verfügung zu stellen.
- Pflicht zur Einhaltung von IT-Sicherheitsstandards besteht *zwei Jahre nach Inkrafttreten der Verordnung*.

Standards „geforderter Sorgfalt“



- **Stand der Technik → Bsp. IT-SiG**
  = fortschrittliche Verfahren, Einrichtungen oder Betriebsweisen, die in der Praxis geeignet erscheinen, die bestmögliche Begrenzung von Gefahren zum Schutz der Allgemeinheit zu sichern. Entscheidend dabei ist, dass die technische Erprobung in einem Fall genügt

- **allgemein anerkannte Regeln der Technik**
  = technische Verfahren und Vorgehensweisen, die in der praktischen Anwendbarkeit erprobt sind und von der Mehrheit der Fachleute anerkannt werden. (z.B. DIN-Normen)

WAS bedeutet "Stand der Technik„ im IT-SiG?

O-Ton: „Das, was das BSI dafür hält!“

- *"Stand der Technik" ist ein gängiger juristischer Begriff:*
  - Bewährtes Instrument (produkt- / verfahrensoffen), da technische Entwicklung immer schneller als Gesetzgebung (vgl. § 3 Abs. 6 S. 1 BImSchG)
  - Nicht allgemeingültig zu beschreiben, konkrete Fallgestaltung maßgeblich
  - *Organisatorische und technische Vorkehrungen* sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Kritischen Infrastruktur steht:
    - angemessen / soll eingehalten werden (BSIG)
    - zumutbar / muss berücksichtigt werden (TMG)
    - angemessen / ist zu berücksichtigen (TKG)
  - Anhaltspunkte: z.B. existierende nationale oder internationale Standards wie DIN oder ISO-Standards oder erfolgreich in der Praxis erprobte Vorbilder für den jeweiligen Bereich (BSI-Grundschutz; ISIS12; ISA+)
  - → retrospektive Betrachtung durch Justiz in Konfliktszenarien zu erwarten!

ICS-Komponente	Sicherheitsrelevante Beobachtungen
Netz	• Anbindung unbekannter Systeme zur Datensicherung
Firewall/ Router	• Regeln nicht ausreichend restriktiv • undokumentierte Regeleinträge • offenbar nicht mehr benötigte Datenflüsse • Bypass im Routing • IP-Forwarding auf Servern
Modems	• ungeschützter Zugang • Anschluss nicht dokumentiert • ständige Verbindung (always-on)
Fernwartung	• Anschluss direkt in Feldebene
Betriebssysteme/ Härtung	• Betriebssystemkomponenten nicht gehärtet • nicht benötigte Dienste angeboten • Nicht-unterstütze neue Betriebssystem- Version und fehlende Patches
Funkverbindungen	• fehlende Verschlüsselung • veraltete Netzelemente
Industrie-Switche	• fehlende Robustheit gegen unerwartete bzw. nicht-standardkonforme Kommunikation • Backdoors (z. B. hardcodierte Passwörter)
veraltete Netzelemente	• Administrativer, webbasierter Zugang ohne Absicherung (z. B. SSL) Fehlende Protokollunterstützung (z. B. nur 'telnet'-Zugang)

BSI, ICS-Security-Kompendium

Meldepflicht bei Sicherheitsvorfällen(§ 8b Abs.4 BSIG)

Zu melden sind: *„… erhebliche Störungen …, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit … führen können oder bereits geführt haben“*

- BSI: das, was für andere Anwender relevant ist – Gesprächskreise diskutieren
- Anonyme (pseudonymisierte) Meldung möglich, solange kein tatsächliche(r) Ausfall / Beeinträchtigung, bei Störfall personalisiert
- BSI: Freiwilligkeit wäre besser, funktioniert(e) aber nicht
- Unbestimmtheit „Störung / Beeinträchtigung“ - welche IT-Sicherheitsvorfälle?
- Wie Vorfälle entdecken, welche Daten werden dazu wie gesammelt?
- Über welchen Meldeweg, in welcher Qualität und Detailtiefe und innerhalb welchen Zeitraums ? Für Banken gem. BaFin nach 1 Stunde
- …

Sanktionen im IT-SiG

Ordnungswidrigkeiten, § 14 BSIG:

- Bußgelder kamen er spät ins Gesetz (→ keine Idee des BSI, das nie Aufsichtsbehörde war und auch nicht sein will!)
- Voraussetzungen:

➢ Vorkehrung nicht / nicht richtig / nicht vollständig / nicht rechtzeitig getroffen
➢ Nicht / nicht rechtzeitige Benennung einer Kontaktstelle
➢ Meldung nicht / nicht richtig / nicht vollständig / nicht rechtzeitig gemacht

→ **Geldbuße bis zu 50.000 €**

➢ Vollziehbarer Anordnung zuwiderhandeln

→ **Geldbuße bis zu 100.000 €**

Bußgelder bei Telemedien, § 16 Abs. 2 Nr. 3 TMG:
→ Geldbuße bis zu 50.000 €

Umsetzungsaufwand

- **Bürokratiekosten** sehr unterschiedlich eingeschätzt
- **Gesetzesbegründung:**
  - 2.000 KRITIS-Betreiber, max. 7 Meldungen pro Betreiber pro Jahr
  - Zeitaufwand pro Meldung: 11 Stunden bei einem Stundensatz von 60 €

    → 660 € pro Meldung
  - Erfüllungsaufwand der Meldepflicht insgesamt: 9,24 Mio. € p.a.
- KPMG-Studie 2013 sowie Studie des Bundesverbands der Deutschen Industrie (BDI) : EUR 1,1 Milliarden p.a. (nur Meldepflicht)
- **Konsequenzen**:

→ Es kommt einiges auf Wirtschaft und öffentliche Institutionen zu

→ Besser früher als später beginnen (trotz verfassungsrechtlicher Bedenken)

Fazit

- Betroffenheit prüfen: ITSiG ist mehr als KRITIS - betrifft Unternehmen und öffentliche Einrichtungen, Zulieferer, Website-Betreiber, SaaS u.a.
- IT-Sicherheit ist Risikomanagement (Sphäre der Unternehmens- / Behördenleitung) und Haftungstatbestand gegenüber Kunden
- Schutzbedarfsanalyse durchführen + dokumentieren
- Stand der Technik maßgeblich: ermitteln + umsetzen
- Einführung, Betrieb und kontinuierliche Weiterentwicklung eines ISMS; Ernennung eines ISB
- IT-Sicherheit ist vertraglich zu vereinbaren (Leistungen + Haftung):
  - Jeden Dienstleister für KRITIS-Unternehmen können mittelbar IT-SiG-Pflichten treffen!
  - Wird nichts vereinbart, muss Kunde selbst dazu in der Lage sein - BSI interessiert sich nicht für Dienstleister / Produkte, sondern fordert Maßnahmen direkt beim Pflichtigen ein!

Wird die digitale Infrastruktur Deutschlands nun sicher?

EU Netz- und Informationssicherheitsrichtlinie

- **Inhalt:**
  - Entwicklung nationaler NIS-Strategien durch Mitgliedsstaaten
  - IT-Notfallteams (CERT) in den Mitgliedsstaaten → Kooperationsnetz
  - Harmonisierte Mindeststandards für KRITIS
  - Meldepflicht für KRITIS-Betreiber
- **Kritik / Offene Fragen:**
  - Keine anonyme Meldung (←→ IT-SiG)
  - Nur Mindestharmonisierung, d.h.
    - Europäischer „Flickenteppich“ wahrscheinlich
    - Ggf. Wettbewerbsnachteil für dt. Unternehmen, da IT-SiG strenger (Bsp. Verschlüsselung bei personalisierten Telemedien)
- **Ggf. doppelter Umsetzungsbedarf**: IT-SiG und Inform.sich.RL EU
- Sept. 2015: Weitere Trilog-Verhandlungen: Anwend.bereich noch umstritten
- Dez. 2015: Abschluss und Verabschiedung geplant; Inkrafttr. 20 T.nach Veröff.
- Umsetzung in den Mitgliedsstaaten binnen 18 Mon.

Ausblick II

Entwurf des Bayerischen E-Government-Gesetzes (BayEGovG-E v. 14.07.2015, LT-Drs.17/7537)

- Sicherheit der informationstechnischen Systeme der Behörden ist *im Rahmen der Verhältnismäßigkeit* sicherzustellen
  - Behörden haben zu diesem Zweck die technischen und organisatorischen Maßnahmen zu treffen und
  - die hierzu erforderlichen Informationssicherheitskonzepte zu erstellen (vgl. Art. 8 Abs. 1 BayEGovG-E).
- Verpflichtungen gelten für die öffentlich-rechtliche Verwaltungstätigkeit der Gemeinden und damit auch für öffentlich-rechtlich handelnde Wasserversorger (vgl. Art. 1 Abs. 1 BayEGovG-E).
- BayEGovG-E in Kommentarform zum Download unter http://bayrvr.de/wp-content/uploads/BayEGovG-Entwurf_Kommentar.doc

Kontakt

Fragen - Schulungsbedarf?

LMU München
Rechtsinformatikzentrum
Prof.-Huber-Platz 2
80539 München

Thomas.Hofer@lmu.de
089 / 2180-2752