Bundesverband

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Allianz für Sicherheit der Wirtschaft e.V. - ASW Bundesverband

TeleTrusT/ASW-Workshop "IT-Sicherheit in der Wirtschaft"

Berlin, 23.09.2015

IT-Sicherheitsgesetz

Dr. Markus Dürig, Bundesministerium des Innern

Bundesministerium
des Innern

Gliederung

- Internetnutzung
- Cyber-Angriffe
- Cybersicherheitslage
- Vertrauen in die Nutzung des Internets
- Cybersicherheitsstrategie der Bundesregierung
- Digitale Agenda der Bundesregierung
- IT-Sicherheitsgesetz

Internetnutzung

- Mehr als 2,7 Mrd. Menschen nutzen heute das Internet (Steigerung in den letzten 10 Jahren: 400%)
- 80% der Bürgerinnen und Bürger in Deutschland sind regelmäßig im Internet unterwegs (EU: 72%)
- 90% der unter 30jährigen sind in sozialen Netzwerken aktiv
- 40% der Wertschöpfung weltweit basiert schon heute auf der Informations- und Kommunikationstechnologie
- 50% der Unternehmen in Deutschland sind vom Internet abhängig
- IT-Steuerung von globaler Produktionsteilung, Steuerung von Geschäftsprozessen
- Sichere und solide Informationsinfrastrukturen sind ein Standortfaktor mit Zukunft

Bundesministerium des Innern

Cyberangriffe

Ungerichtete Angriffe

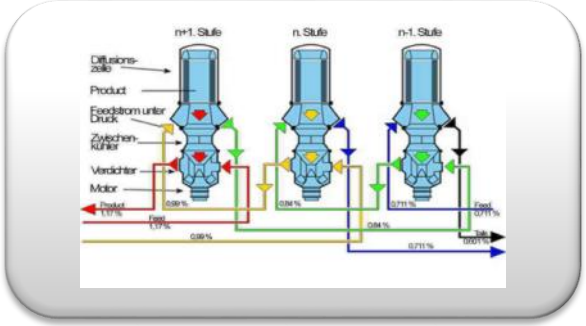
- Sabotage, Betrug, etc.
- Unspezifische Zielgruppen
- **SPAM, Viren, Würmer, Trojaner, Drive-by-Downloads**

Gezielte Angriffe

- Spionage und Sabotage
- Spezielle Zielgruppen
- **Social-Engineering + Trojaner**

Skalpellartige Angriffe

- Sabotage spezieller IT-Systeme (und Infrastrukturen) mit großem Schadensausmaß
- Komplexe, langwierige Vorbereitung
- **Zero-Day-Verwundbarkeiten**
- **Fälschung von Zertifikaten**



Bundesministerium
des Innern

Cybersicherheitslage – Überblick I

Schwachstellen

- 2014: rund 700 kritische Schwachstellen in den meistverbreiteten Softwareprodukten, allein im ersten Halbjahr fünf bekannt gewordene Zero-Day-Schwachstellen

Schadprogramme

- Gesamtzahl der PC-basierten Schadprogrammvarianten: mehr als 250 Millionen
- Zahl der Schadprogrammvarianten steigt täglich um rund 300.000
- Jeden Monat allein in Deutschland mindestens 1 Million Infektionen durch Schadprogramme

Botnetze

- In Deutschland sind mehr als 1 Million Internetrechner Teil eines Botnetzes

Bundesministerium
des Innern

Cybersicherheitslage – Überblick II

Identitätsdiebstahl

- Täglich werden mehrere Tausend digitale Identitäten gestohlen
- BSI analysiert monatlich 11.000 neue Schadprogramme mit Bezug zu Identitätsdiebstahl in Deutschland

DDoS

- 2014: allein in Deutschland über 32.000 DDoS-Angriffe
- Mehr als ein Drittel der Unternehmen war in den letzten drei Jahren Ziel eines DDoS-Angriffs auf ihre Webseiten
- Ein Viertel der Unternehmen war von DDoS-Angriffen auf die Netzinfrastruktur betroffen.

Bundesministerium
des Innern

Cybersicherheitslage – Überblick III

Regierungsnetze/Bundesverwaltung/Parlament

- Täglich tausende ungezielter Angriffe auf das Regierungsnetz
- Durch spezielle Sicherheitsmaßnahmen werden monatlich zusätzlich bis zu 60.000 verseuchte E-Mails in den Netzen der Bundesverwaltung abgefangen
- 2014: täglich 15 bis 20 hochwertige Angriffe auf das Regierungsnetz
- durchschnittlich ein gezielter Angriff pro Tag mit nachrichtendienstlichem Hintergrund

- 2015: Angriff auf IT-Netz des Deutschen Bundestages

Bundesministerium
des Innern

Bekannte Fälle der letzten Jahre

- Juni 2010: IRN, **Stuxnet**– 5 unbekannte Lücken in MS, 2 gestohlene Sicherheitszertifikate, umfangreiche Programmierung
- August 2012: KAT, **Shamoon**– Festplatten von 30.000 Rechnern von Saudi Aramco gelöscht
- Oktober 2012, März 2013: USA, Mehrfach **DDoS-Attacken** auf Banken
- März 2013: USA, Starke **DNS-DDoS-Attacke** auf Anti-Spam-Organisation Spamhaus
- März 2013: KOR, Ausfall der IT-Netzwerke von Banken, Fernsehsendern, Nachrichtenkanälen, wahrscheinlich Cyber-Angriff
- Juni 2013: KOR, Ausfall von Internetpräsenzen zahlreicher staatlicher Stellen und Medien, Vermutlich Cyber-Angriff
- Sep. 2013: DEU, Abfluss von Stammdaten von 2 Mio. Kunden nach Cyber-Angriff
- Dezember 2013: GB, Software-Fehlfunktion in Flugsicherheitszentrale, Ausfall von rund 200 Flügen in London
- Anfang 2014: DEU, **34 Mio. digitale Identitäten gestohlen**
- Mai 2015: Cyber-Angriff auf den Deutschen Bundestag
- Juni 2015: Autozulassungsstellen in 2 Bundesländer (Hessen/Rheinlandpfalz) angegriffen, sicherheitshalber die Sever vom Netz genommen
- Juni 2015 : Cybervorfall bei der polnischen Fluggesellschaft LOT, Flughafen Warschau keine Starts

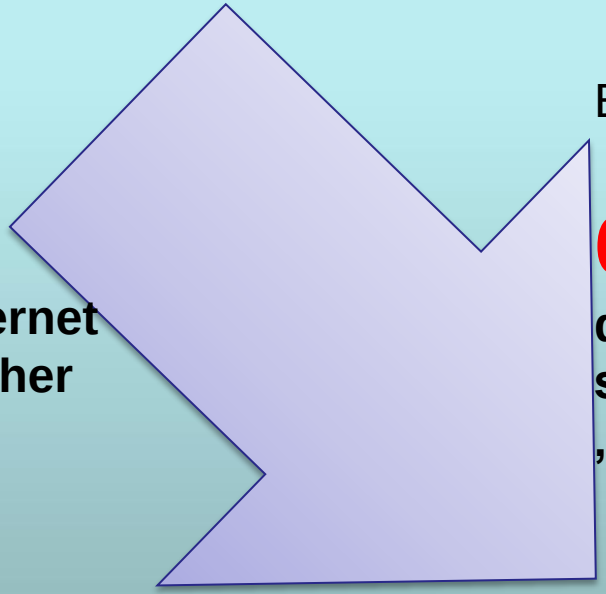
Bundesministerium
des Innern

Das Vertrauen in die Nutzung des Internets sinkt

DIVSI-Umfrage:

39%

fühlen sich im Internet unsicherer als vorher



BITKOM-Umfrage:

66%

der Befragten fühlen sich im Netz „eher“ oder „völlig“ unsicher

„Digitale Sorglosigkeit“

- Konkrete Schutzmaßnahmen werden nur geringfügig häufiger umgesetzt
- z.B. E-Mail-Verschlüsselung oder Basis-Sicherheitsmaß-nahmen wie Patch-Management bei Smartphones werden kaum genutzt
- Grund: Verlust an Komfort und Bedienbarkeit
- Insbesondere KMU häufig auch gegen einfache Angriffe nur unzulänglich geschützt
- Unternehmen investieren weniger als 5% des IT-Budgets in IT-Sicherheit
- „Social Engineering“ auf dem Vormarsch – Bedeutung des Anwenderverhaltens

Bundesministerium
des Innern

Cybersicherheitsstrategie der Bundesregierung 2011

Feb. 2011

- Cyber-Sicherheitsrat
- Nationales Cyber-Abwehrzentrum
- Kritische IT-Infrastrukturen
- IT der Bürger
- IT des Staates
- Einsatz verlässlicher Informationstechnologie
- Internationale Zusammenarbeit
- Abwehr von Cyber-Angriffen
- Wirksame Kriminalitätsbekämpfung
- Personalentwicklung der Bundesbehörden

Bundesministerium
des Innern

Kritische IT-Infrastrukturen

- Stärkung UP K ab 2011
  - ➢ Vertiefung der kooperativen Zusammenarbeit mit kritis-Wirtschaft im UP K
    aber: kaum Meldung von IT-Sicherheitsvorfällen
    manche Sektoren nur partiell abgedeckt
    kein Lagebild DEU möglich
- Kritis-Gespräche 2012
  - ➢ Gesprächsreihe des Bundesinnenministers Dr. Friedrich mit Vertretern aller Sektoren der kritischen Infrastrukturen 2012

Bundesministerium
des Innern

Koalitionsvertrag der Bundesregierung 2013

- „Wir schaffen ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle."
- „Wir bauen die Kapazitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auch des Cyber-Abwehrzentrums aus."
- „Die Bundesbehörden werden verpflichtet, zehn Prozent ihrer IT-Budgets für die Sicherheit ihrer Systeme zu verwenden."
- „Um zu gewährleisten, dass die Nutzerinnen und Nutzer über die Sicherheitsrisiken ausreichend informiert sind, sollen Internetprovider ihren Kunden melden, wenn sie Hinweise auf Schadprogramme oder ähnliches haben."

Bundesministerium
des Innern

Digitale Agenda der Bundesregierung 2014

Handlungsfelder

- Digitale Infrastruktur und Breitbandausbau,
- Digitale Wirtschaft,
- Innovativer Staat,
- Digitale Gesellschaft, Forschung, Bildung und Kultur,
- **Sicherheit**,
- Schutz und Vertrauen für Gesellschaft und Wirtschaft sowie
- Europäische und Internationale Dimension der Digitalen Agenda.

=> IT-Sicherheit als zentrales Querschnittsthema

Bundesministerium
des Innern

IT-Sicherheitsgesetz – vier Ziele

- **Schutz der IT kritischer Infrastrukturen**
  IT-Mindeststandards und Meldepflichten für Kritische Infrastrukturen - §§ 8a bis 8d BSIG sowie Spezialgesetze AtomG, EnWG und TKG

- **Steigerung der Sicherheit im Internet**
  Anhebung des allgemeinen IT-Sicherheitsniveaus für Telekommunikationsnetze und Telemediendienste

- **Stärkung von BSI, BKA und BNetzA**

- **Verbesserung des Schutzes der Bundesbehörden**

Bundesministerium
des Innern

IT-Sicherheitsgesetz
- Definition kritische Infrastrukturen

„Einrichtungen, Anlagen oder Teile davon , die den Sektoren Energie, Informations-technik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz-und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit eintreten würden.“

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Ver-sicherungswesen

- Medien und Kultur
- Staat und Verwaltung

Bundesministerium
des Innern

IT-Sicherheitsgesetz – KRITIS-Schutz I

- **Pflicht zur Einhaltung von IT-Mindestsicherheitsstandards und Audits**
  - angemessene organisatorische und technische Vorkehrungen
  - zur Vermeidung von Störungen der informationstechnischen Systeme, Komponenten und Prozesse
  - die für die Funktionsfähigkeit der kritischen Infrastrukturen maßgeblich sind;
  - Stand der Technik soll eingehalten werden;
  - Erarbeitung durch die Branchen (kooperativer Ansatz);
  - Anerkennung durch BSI, wenn geeignet zur Gewährleistung der Anforderungen;
  - Regelmäßige Audits mindestens alle zwei Jahre gegenüber BSI nachzuweisen; BSI kann Beseitigung von Sicherheitsmängeln verlangen;
  - BSI kann Anforderungen an die Durchführung der Audits und Meldungen festlegen.

Bundesministerium
des Innern

IT-Sicherheitsgesetz – KRITIS-Schutz II

- **Pflicht zur Meldung von erheblichen Störungen** der informationstechnischen Systeme, Komponenten und Prozesse, die zu einem Ausfall/Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastruktur führen können/geführt haben

  - Pseudonymisierte Meldung möglich, wenn noch keine Beeinträchtigung von kritis
  - Nennung des Unternehmens nur bei Schadenseintritt in kritis
  - Einbindung der sonst zuständigen Aufsichtsbehörden
  - Auswertung und Warnung/Information der zuständigen Stellen und der KRITIS-Betreiber bei möglich Betroffenheit

Bundesministerium
des Innern

IT-Sicherheitsgesetz – KRITIS-Schutz III

- **Bereichsausnahmen**
  - Vorrang von Spezialgesetzen mit analogem Schutzniveau
  - daher Regelungen im EnWG, TKG, AtomG
  - Weitere Ausnahmen möglich

- **Absicherung der Informationen beim BSI**
  - Auskunft an Dritte nur, wenn schutzwürdige Interessen des Betreibers und Sicherheitsinteressen nicht entgegen stehen
  - Keine Akteneinsicht
  - Kein Auskunftsrecht nach dem Informationsfreiheitsgesetz

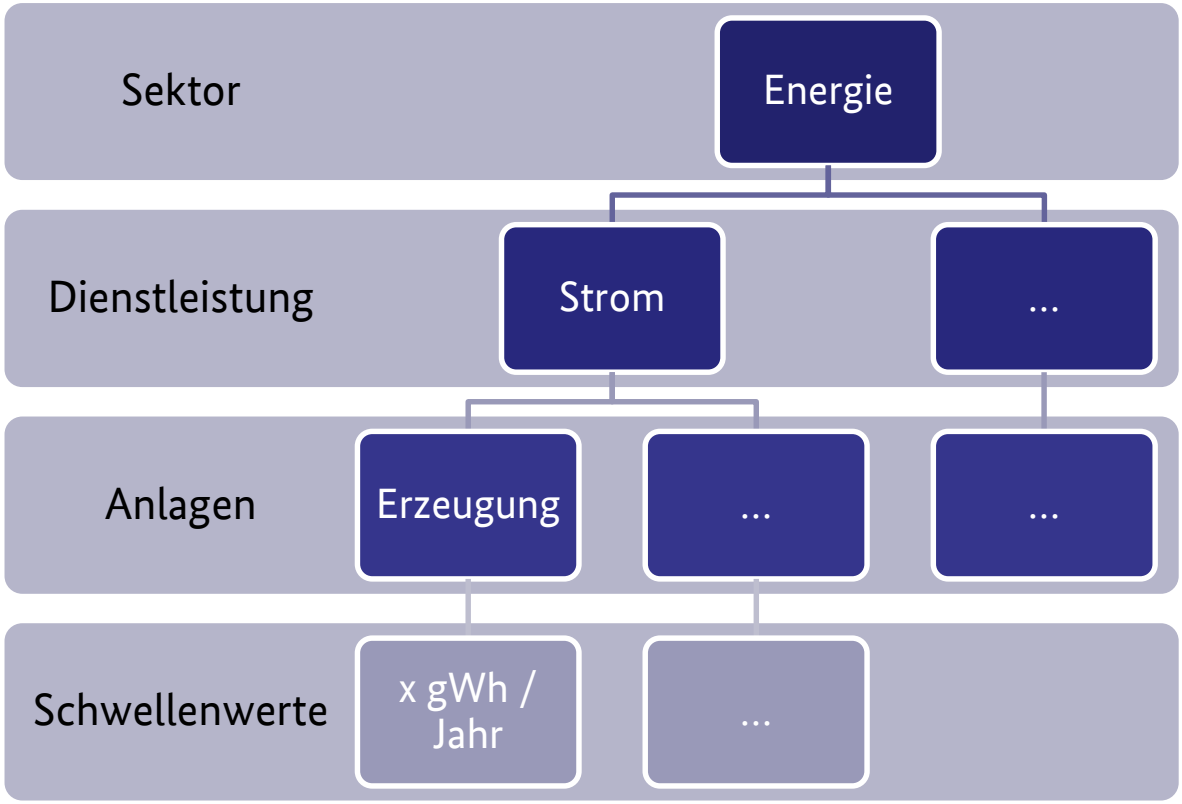
- **Sanktionsbefugnisse des BSI gegen kritis-Betreiber**

Bundesministerium des Innern

BSI-KritisV - Vorgehensweise

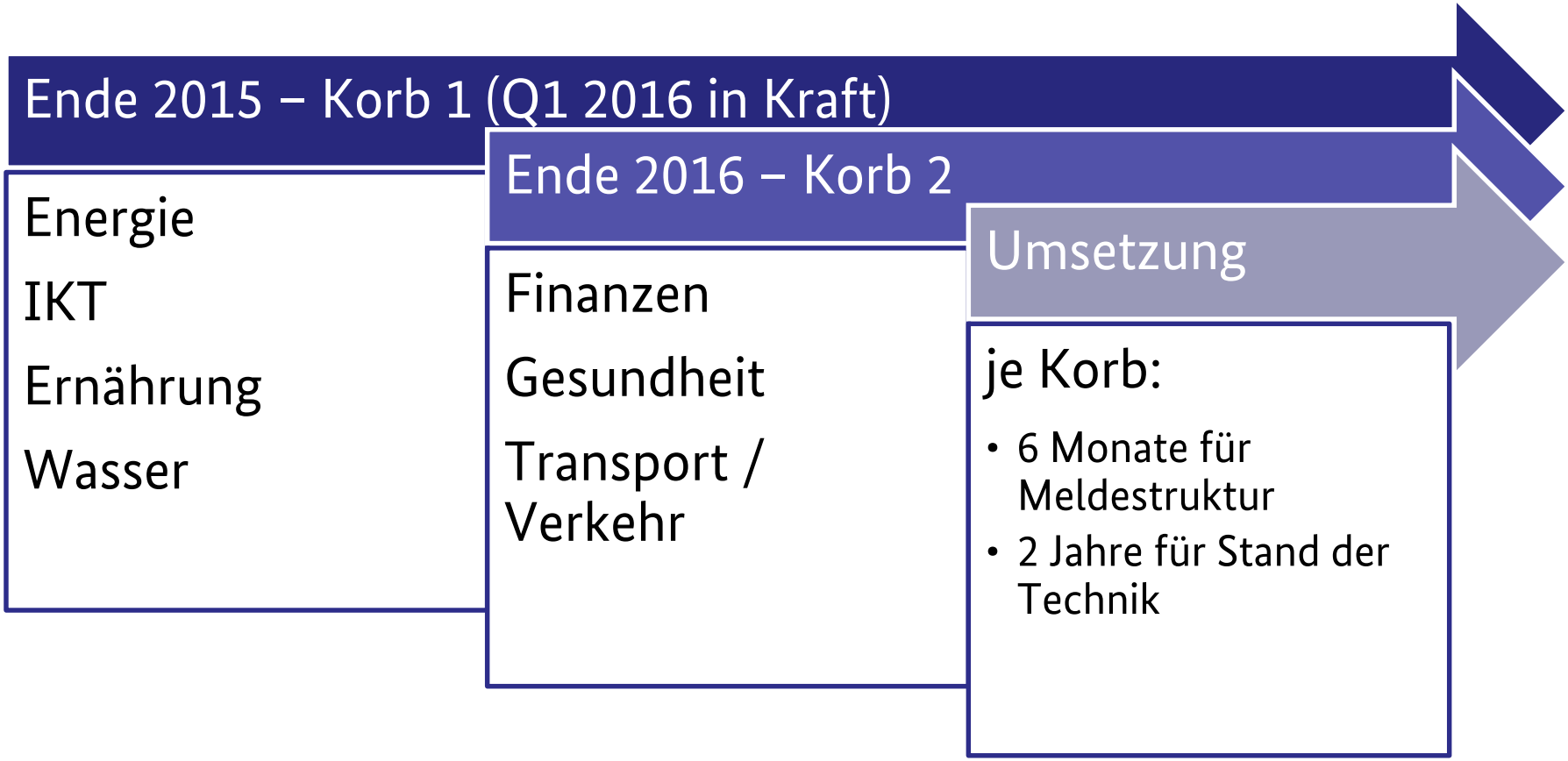
Versorgung der Gesellschaft mit wichtigen Dienstleistungen

1. **Qualität**: Dienstleistungen in den KRITIS-Sektoren, die für die Versorgungskette relevant sind und abstrakte Anlagen
2. **Quantität**: Schwellenwerte innerhalb dieser Dienstleistungen



Bundesministerium des Innern

Zeitplanung



Bundesministerium
des Innern

IT-Sicherheitsgesetz –Sicherheit im Internet

- TK-Diensteanbieter: „Stand der Technik“ zum Schutz gegen unerlaubte Zugriffe auf die TK- und Datenverarbeitungs-systeme

- Pflicht zu Information der Kunden bei Angriffen auf Kundensysteme plus Hinweise auf mögliche Wege zur Beseitigung

- Höheres Schutzniveau bei Telemedienanbietern („Stand der Technik berücksichtigen“) gg. unerlaubte Zugriffe und zum Schutz personenbezogener Daten und zur Sicherung gg. Störungen durch äußere Angriffe.

Bundesministerium
des Innern

IT-Sicherheitsgesetz – Stärkung der BNetzA

- Stärkere Überprüfung des Sicherheitskonzepts der TK-Anbieter durch BNetzA alle zwei Jahre

Bundesministerium
des Innern

IT-Sicherheitsgesetz – Stärkung des BSI

- BSI-als internationale Zentralstelle
- Ausbau der Warnbefugnisse (auch bei Datenverlust und unerlaubtem Zugriff auf Daten)
- Befugnisse zur Untersuchung von IT-Produkten die auf dem Markt bereitgestellt werden im Rahmen der gesetzlichen Aufgaben des BSI (Schutz der BdVw, der IT der kritis-Betreiber und der Beratung und Warnung vor Sicherheitsmängeln)
- Stärkere Rolle bei Erstellung des TK-Sicherheitskataloges
- jährlicher Bericht zur Lage der IT- und Cyber-Sicherheit in DEU

Bundesministerium
des Innern

IT-Sicherheitsgesetz – Stärkung des BKA

Erweiterung der Ermittlungszuständigkeiten des BKA

bisher	Computersabotage u.a. bei lebenswichtigen Einrichtungen
künftig	Sämtliche Computerdelikte Angriffe auf alle Einrichtungen des Bundes

Bundesministerium
des Innern

IT-Sicherheitsgesetz - Verbesserung des Schutzes der IT der Bundesbehörden

- Pflicht der Bundesbehörden, dem BSI Zugang zu ihren behördeninternen Portokoll- und Schnittstellendaten zu gewähren
- Befugnis für das BMI, vom BSI erarbeitete Mindeststandards für die IT-Sicherheit des Bundes als Verwaltungsvorschrift zu erlassen im Benehmen (vorher: Einvernehmen) mit dem Rat der IT-Beauftragten der Ressorts

Bundesministerium
des Innern

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Markus Dürig
Bundesministerium des Innern
Leiter Referat IT II 1 –
Grundsatzangelegenheiten IT- und Cybersicherheit; Schutz im Cyberraum; Cyberabwehrzentrum

Alt-Moabit 140
10557 Berlin

Tel.: 030 18 681 11374
E-Mail: ITII1@bmi.bund.de