



TeleTrust
Pioneers in IT security.

Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrust, bevh und BISG

Berlin, 29.11.2016

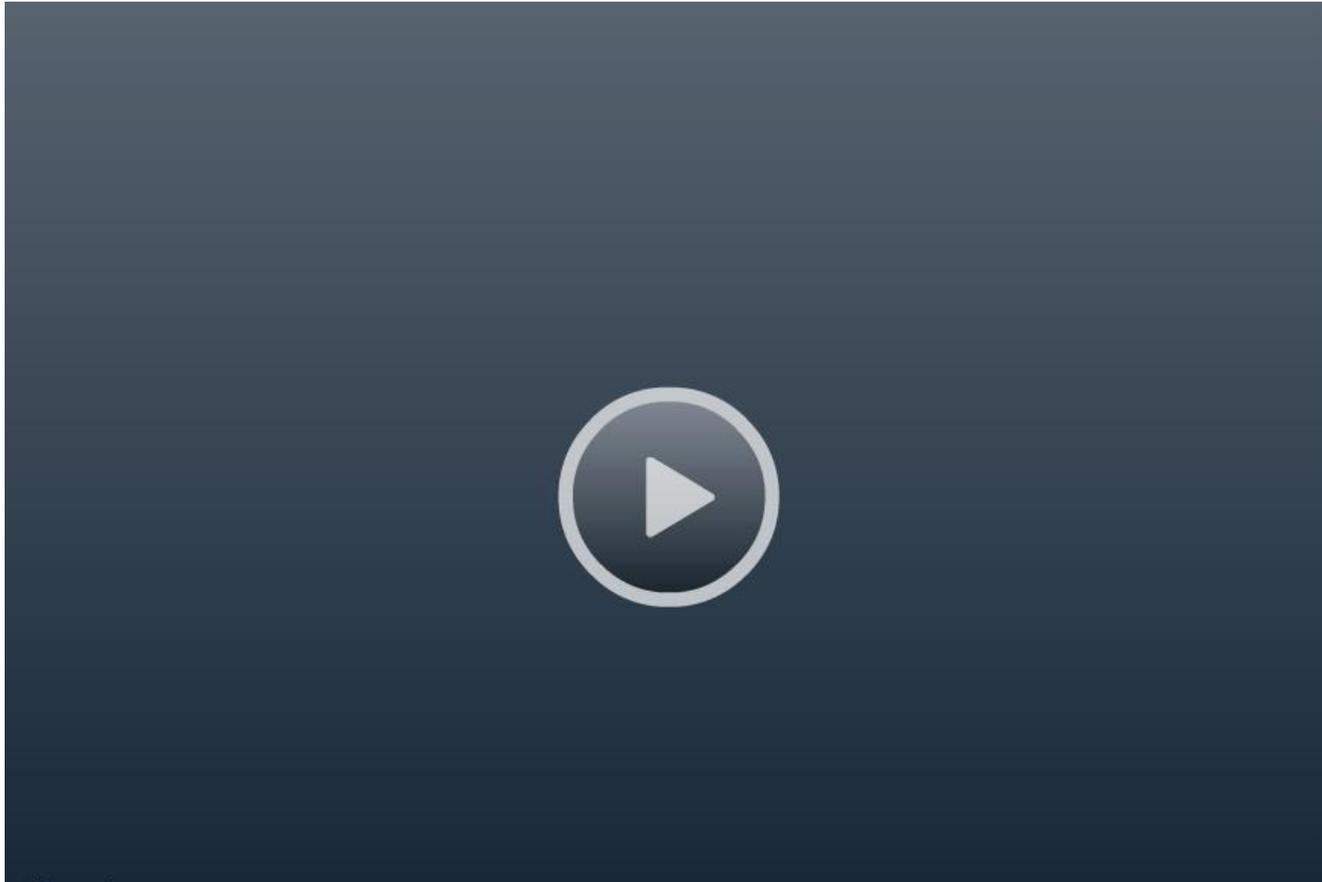
Nihil Novi?

Praktische Umsetzung der Reporting- Anforderungen aus dem ITSiG

Dr. Aleksandra Sowa

Deutsche Telekom AG

Security Incident Reporting gem. Art. 13a (EU)



Art 13a - Annual incidents report:results video

Major incidents in the electronic communications sector: Results of the 2012 report

Duration: 2013

Year: [Incident Reporting](#)

Tags:

Embed:

<https://www.enisa.europa.eu/media/multimedia/art-13a-annual-incident-report-results-screencast>

DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2009

amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

THE EUROPEAN P
Having regard to the
Having regard to the
Having regard to the
Having regard to the
Acting in accordance

'CHAPTER IIIa SECURITY AND INTEGRITY OF NETWORKS AND SERVICES

Article 13a

Security and integrity

1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.

3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

4. The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements. These technical implementing measures shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraphs 1 and 2.

These implementing measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 22(3).

RICHTLINIE 2009/140/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

18.12.2009

DE

Amtsblatt der Europäischen Union

L 337/37

RICHTLINIE 2009/140/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 25. November 2009

zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste

„KAPITEL III A

SICHERHEIT UND INTEGRITÄT VON NETZEN UND DIENSTEN

Artikel 13a

Sicherheit und Integrität

(1) Die Mitgliedstaaten stellen sicher, dass Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, angemessene technische und organisatorische Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten ergreifen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen für Nutzer und zusammengeschaltete Netze zu vermeiden und so gering wie möglich zu halten.

(2) Die Mitgliedstaaten stellen sicher, dass Unternehmen, die öffentliche Kommunikationsnetze bereitstellen, alle geeigneten Maßnahmen ergreifen, um die Integrität ihrer Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen.

(3) Die Mitgliedstaaten stellen sicher, dass Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, der zuständigen nationalen Regulierungsbehörde eine Verletzung der Sicherheit oder einen Verlust der Integrität mitteilen, die bzw. der beträchtliche Auswirkungen auf den Betrieb der Netze oder die Bereitstellung der Dienste hatte.

Gegebenenfalls unterrichtet die betroffene nationale Regulierungsbehörde die nationalen Regulierungsbehörden der anderen Mitgliedstaaten und die Europäische Agentur für Netz- und Informationssicherheit (ENISA). Die betroffene nationale Regulierungsbehörde kann die Öffentlichkeit unterrichten oder die Unternehmen zu dieser Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Verletzung im öffentlichen Interesse liegt.

Einmal pro Jahr legt die betroffene nationale Regulierungsbehörde der Kommission und der ENISA einen zusammenfassenden Bericht über die eingegangenen Mitteilungen und die gemäß diesem Absatz ergriffenen Maßnahmen vor.

(4) Die Kommission kann geeignete technische Durchführungsmaßnahmen zur Harmonisierung der in den Absätzen 1, 2 und 3 genannten Maßnahmen beschließen, einschließlich solcher Maßnahmen, mit denen Umstände, Form und Verfahren der vorgeschriebenen Mitteilungen festgelegt werden, wobei sie weitestgehend die Stellungnahme der ENISA berücksichtigt. Diese technischen Durchführungsmaßnahmen werden so weit wie möglich auf europäische und internationale Normen gestützt; durch diese Maßnahmen werden die Mitgliedstaaten nicht daran gehindert, zusätzliche Anforderungen festzulegen, um die in den Absätzen 1 und 2 dargelegten Ziele zu erreichen.

Diese Durchführungsmaßnahmen zur Änderung nicht wesentlicher Bestimmungen dieser Richtlinie durch Ergänzung werden nach dem in Artikel 22 Absatz 3 genannten Regelungsverfahren mit Kontrolle erlassen.

DAS EUROP
gestützt auf d
auf Vorschlag
nach Stellung
nach Stellung
gemäß dem V

29.11.2016

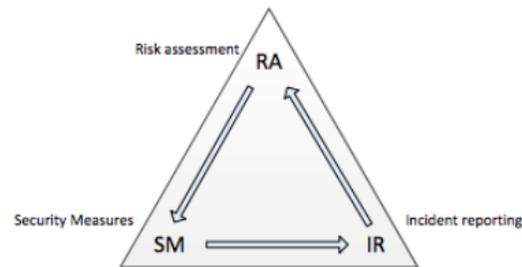
Security Incident Reporting gem. Art. 13a (EU)

- "ENISA Annual Security Report" der European Union Agency for Network and Information Security, ENISA
- Grundlage: Artikel 13a der EU Framework Directive of the Telecom Reform des Telecom Package
- Ergebnisse 2015:
<https://www.enisa.europa.eu/publications/impact-evaluation-article13a>





[Forgot your password?](#)



The three technical guidelines address these three processes. These guidelines are updated frequently, in collaboration with the NRAs. The latest versions can be found at the following links:

- [Article 13a Technical Guideline on Incident Reporting](#): Defines a cross-EU reporting framework and explains different approaches to setting up a national incident reporting process.
- [Article 13a Technical Guideline on Security Measures](#): An overview of a range of different security measures which could be considered by NRAs when assessing compliance to NRAs. These measures were derived from existing international standards (see below).
- [Article 13a Technical Guideline on Threats and Assets](#): Provides a dictionary of threats and assets which aims to support the incident reporting framework and aims to support the review of risk assessment by providers.

Note that the Article 13a guideline on security measures is now subsumed by the [Technical Guideline on Security Measures in Article 4 and Article 13a](#).

GRUPPO TELECOM ITALIA

“ Centro Nazionale Anticrimine Informatico per la protezione delle Infrastrutture Critiche (CNAIPIC) ”

- **The National Crime Centre for Critical Infrastructures Protection is the specialized unit inside the Police Service of Postal and Communication service for the prevention of cyber crimes against critical national infrastructures**
- **The headquarter was established in June 2009 in Rome**
- **It was established by a decree in August 2008**



TELECOM
ITALIA

4

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)



The screenshot shows the homepage of the German Federal Government's Ministry of the Interior. At the top, there are navigation links for 'ENGLISCH', 'NACHRICHTEN', 'PRESSE', 'ÜBERSICHT', 'KONTAKT', 'GEBÄRDENSPRACHE', and 'LEICHTE SPRACHE'. The main header features the German coat of arms and the text 'Bundesministerium des Innern'. A search bar is located on the right. Below the header, there is a navigation menu with categories: 'Ministerium', 'Sicherheit', 'Gesellschaft und Verfassung', 'Moderne Verwaltung und Öffentlicher Dienst', 'IT und Netzpolitik', 'Migration und Integration', 'Bevölkerungsschutz', and 'Sport'. The main content area is titled 'Nachrichten' and features a news article from December 17, 2014, titled 'Bundesregierung beschließt IT-Sicherheitsgesetz'. The article text states: 'Die IT-Systeme und digitalen Infrastrukturen Deutschlands sollen zu den sichersten weltweit werden. Mit dem heute auf Vorschlag von Bundesinnenminister de Maizière beschlossenen Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) liegt eines der ersten konkreten Ergebnisse in Umsetzung der Digitalen Agenda der Bundesregierung vor.' There are two callout boxes on the right side of the screenshot. The top one is titled 'Gesetzentwurf der Bundesregierung zum IT-Sicherheitsgesetz' and includes a 'Download' button (PDF, 270 KB, not barrier-free) and a 'Vorlesen' button (document with ReadSpeaker). The bottom one is titled 'Lagebericht zur IT-Sicherheit' and includes a 'Download' button (PDF, 2 MB, not barrier-free) and a 'Vorlesen' button.

*Source: <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html>
29.11.2016
Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis" gemeinsame Veranstaltung von TeleTrust, bevh und BISG

"Mit diesem Gesetz sind wir europaweit
Vorreiter und Vorbild",
sagte de Maizière bei der Vorstellung des
Gesetzes in der Bundespressekonferenz.
"Es leistet seinen Beitrag dazu, dass das Netz
sicherer wird und die digitalen Infrastrukturen
Deutschlands künftig zu den sichersten weltweit
gehören."

*Source: <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html>

§ 8b

Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

- (1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.
- (2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe
 1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,
 2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,
 3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und

(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 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.

(4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu

§ 8b

Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

Drucksache 18/4096

– 12 –

Deutscher Bundestag – 18. Wahlperiode

einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und 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.

(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.

(6) Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

"Security should not compromise freedom of speech, privacy and integrity of the unified Internet: rather, it should support them"

(Neelie Kroes, 5 February 2012, Munich)