Bundesamt
für Sicherheit in der
Informationstechnik

UP KRITIS

Medienunternehmen als potentielle Angriffsziele aus dem Internet

Dr. Uwe Jendricke
Bundesamt für Sicherheit in der Informationstechnik

EMR/APR-Workshop „Datenschutz und Datensicherheit“
4. Mai 2018
Frankfurt am Main

Vorfälle

- Verschlüsselungstrojaner
- APT
- Mining Malware

4. Krypto-Malware: Missbräuchliches Schürfen von Krypto-Währungen nimmt zu

Der Erfolg von Krypto-Währungen hat zu einem neuen Trend bei Malware geführt: Malware, die heimlich infizierte Rechner zum Schürfen einsetzt. Laut ZDNet merken Verbraucherinnen und Verbraucher in vielen Fällen überhaupt nicht, dass ihre Rechner missbraucht werden. Denn wenn di Prozessoren auf Hochtouren arbeiten und die Lüftung lauter läuft als sonst, ist häufig nicht unmittelbar klar, dass Schadsoftware dahinter steckt. Ihnen selbst entsteht kein unmittelbar spürba Schaden. Anfang März hat sich so eine Krypto-Malware innerhalb weniger Stunden auf fast 500.00 Windows-PCs ausgebreitet, um die Krypto-Währung Electroneum zu schürfen. Ein gut gesicherter Browser zählt zu den grundlegenden Schutzmaßnahmen vor Krypto-Mining und ähnlichen Malware

Risiken

- Sicherheitslücken
- Fehlendes Wissen
- Geringes Sicherheitsbewusstsein
- Alte Software

Foto: Roberta F., https://commons.wikimedia.org/wiki/File:HRT_studio_radio_1_250409.jpg

Bundesamt für Sicherheit in der Informationstechnik

Prozesssteuerungen, spezielle und klassische IT

Prozesssteuerungssysteme (ICS)

Büro-IT

Spezialsysteme

http://ysterografa.gr/wp-content/uploads/2016/08/03_Bild_1_01.jpg

Bundesamt für Sicherheit in der Informationstechnik

Alte Betriebssysteme

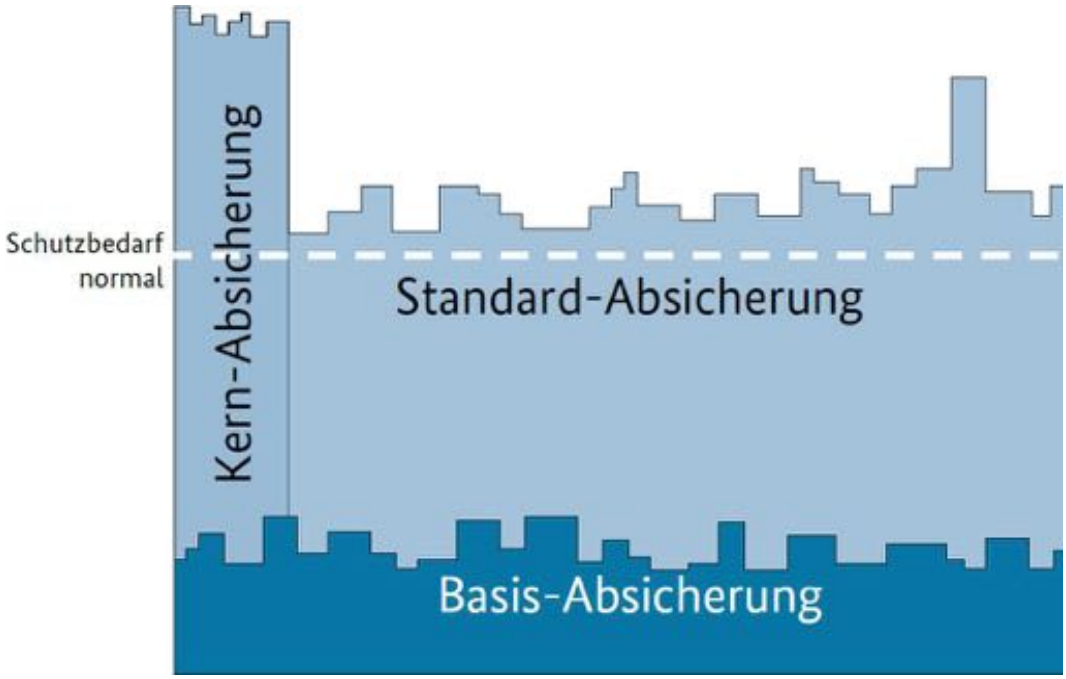
Bundesamt für Sicherheit in der Informationstechnik

Lösungswege

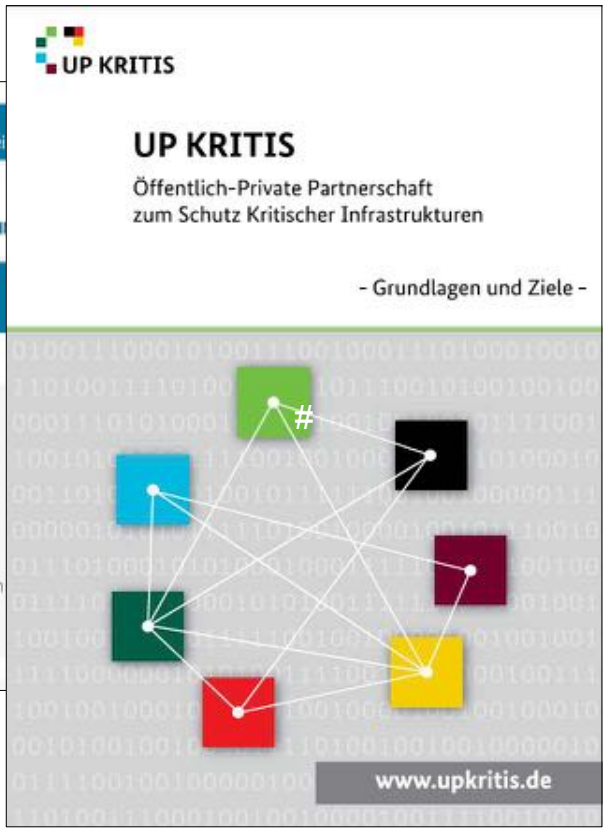
https://www.upkritis.de

https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

Grundschutz / BSI-Standard 200-2



UP KRITIS / Allianz für Cyber-Sicherheit



Kritische Infrastrukturen

- Sektoren -

Bundesamt für Sicherheit in der Informationstechnik

UP KRITIS

- Vision -

gemeinsame Verantwortung von Staat und Wirtschaft

zentraler Beitrag zum Schutz der Kritischen Infrastrukturen

UP KRITIS

Sicherstellung der Versorgung der Bevölkerung

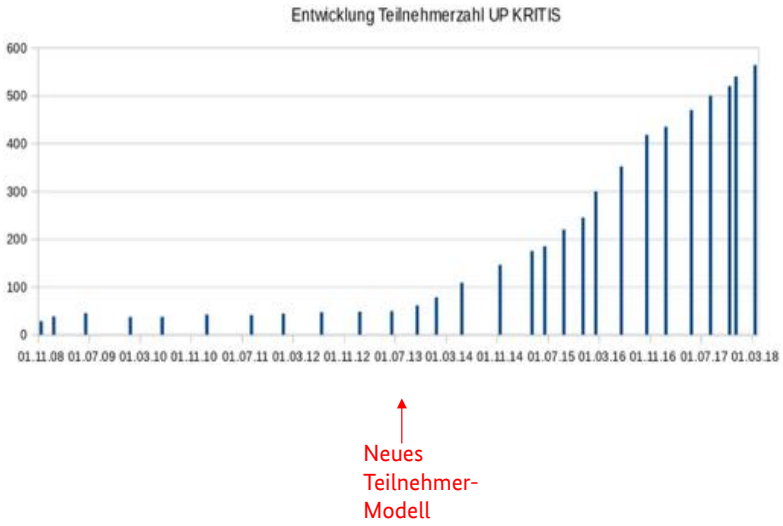
Informationstechnik als Schwerpunkt der Arbeiten

Bundesamt für Sicherheit in der Informationstechnik

UP KRITIS
- Teilnehmer -

Wer kann teilnehmen?

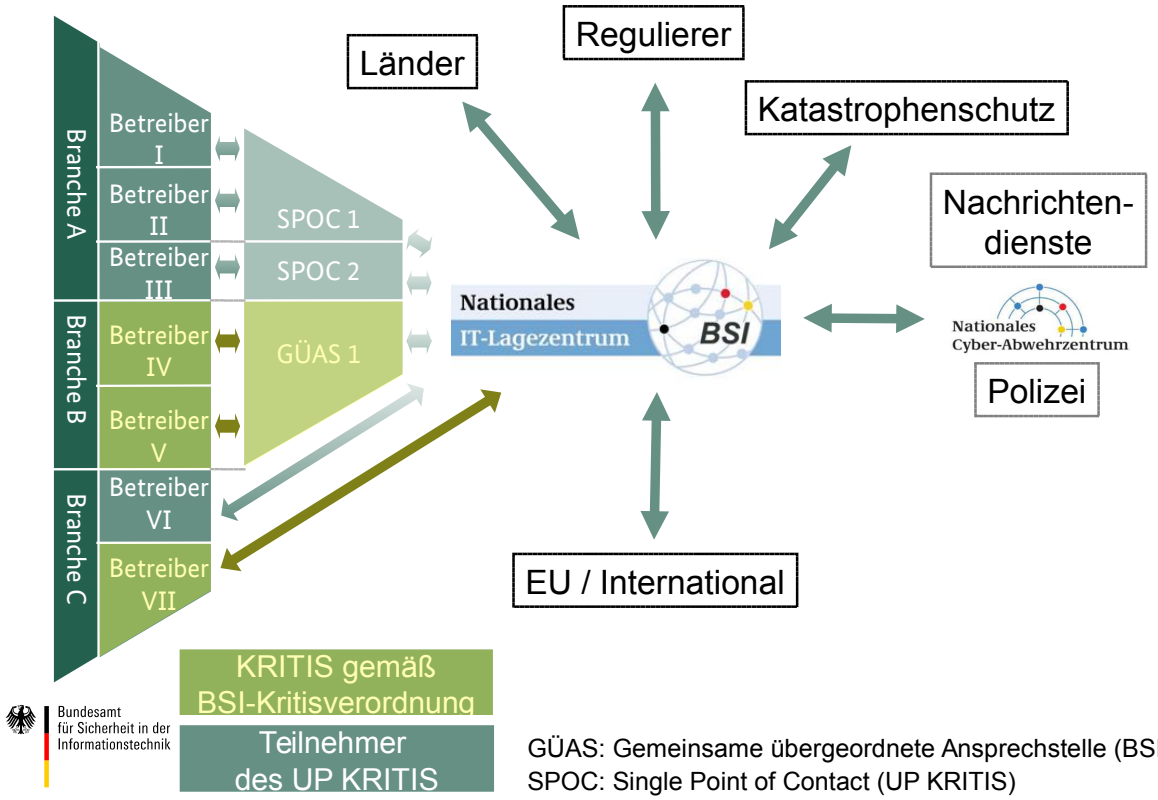
- Alle **Organisationen** mit Sitz in Deutschland, die Kritische Infrastrukturen in Deutschland betreiben
- Nationale **Fach- und Branchenverbände** aus den KRITIS- Sektoren
- Die zuständigen **Behörden**



UP KRITIS
- Ziele -

UP KRITIS

- Operativ: - Vernetzung, Informationsaustausch -



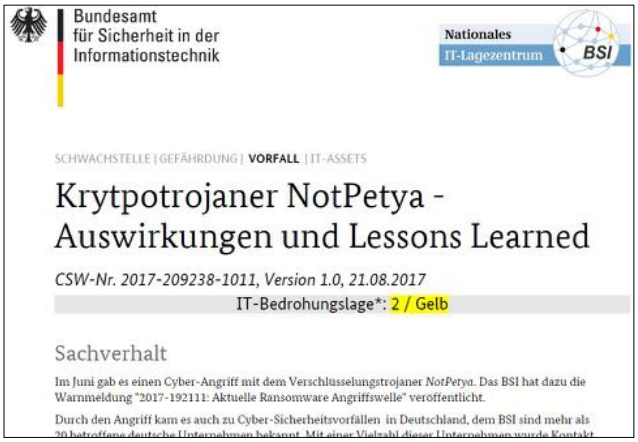
GÜAS: Gemeinsame übergeordnete Ansprechstelle (BSIG)
SPOC: Single Point of Contact (UP KRITIS)

UP KRITIS

- Operativ: Meldewesen -


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

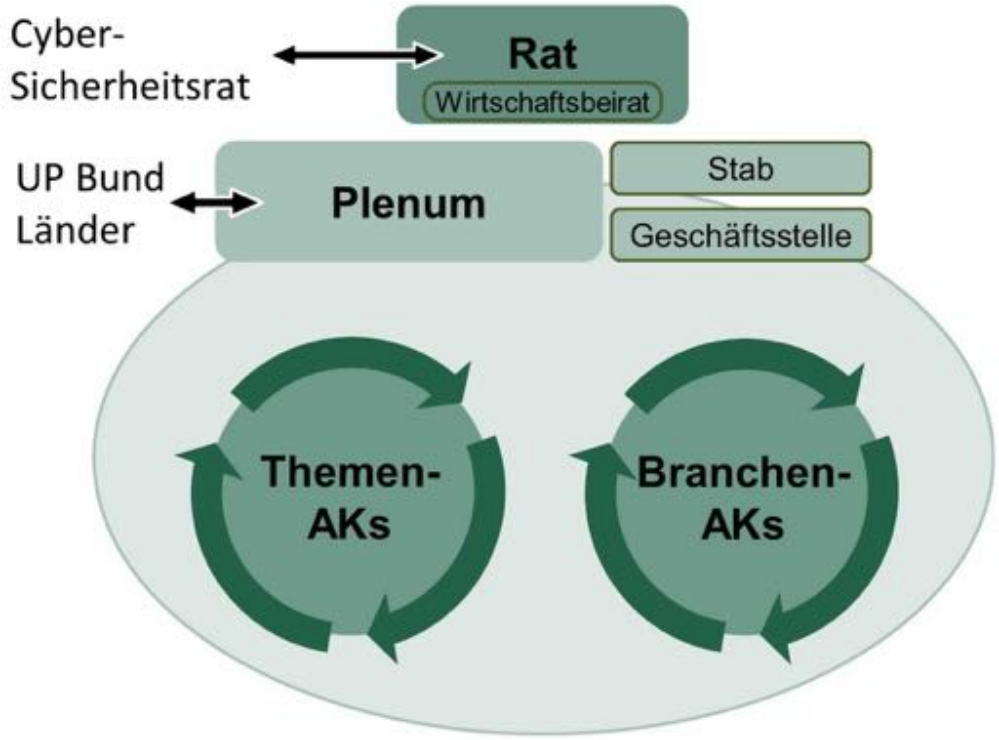
IT-SiG


Bundesamt für Sicherheit in der Informationstechnik
Nationales IT-Lagezentrum BSI
SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS
Krytpotrojaner NotPetya - Auswirkungen und Lessons Learned
CSW-Nr. 2017-209238-1011, Version 1.0, 21.08.2017
IT-Bedrohungslage*: 2 / Gelb
Sachverhalt
Im Juni gab es einen Cyber-Angriff mit dem Verschlüsselungstrojaner NotPetya. Das BSI hat dazu die Warnmeldung "2017-192111: Aktuelle Ransomware Angriffswelle" veröffentlicht.
Durch den Angriff kam es auch zu Cyber-Sicherheitsvorfällen in Deutschland, dem BSI sind mehr als


Bundesamt für Sicherheit in der Informationstechnik
Nationales IT-Lagezentrum
SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS
Gezielter E-Mail-Angriff gegen Medienunternehmen
Ausgeführter Anhang lädt PowerShell Exploit-Framework "Empire" n
CSW-Nr. 2018-174327, Version 1.0, 29.03.2018
IT-Bedrohungslage*: 2 / Gelb
Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Inform gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:
TLP-Amber: Organisationsinterne Verteilung
Informationen in dieser Stufe dürfen innerhalb der Organisation der Empfänger weitergegeben werden, jedoch „Kenntnis nur wenn nötig". Der Informationsersteller muss zusätzlich beabsichtigte Einschränkungen der Weit

UP KRITIS

- Strategisch-Konzeptionelle Zusammenarbeit -



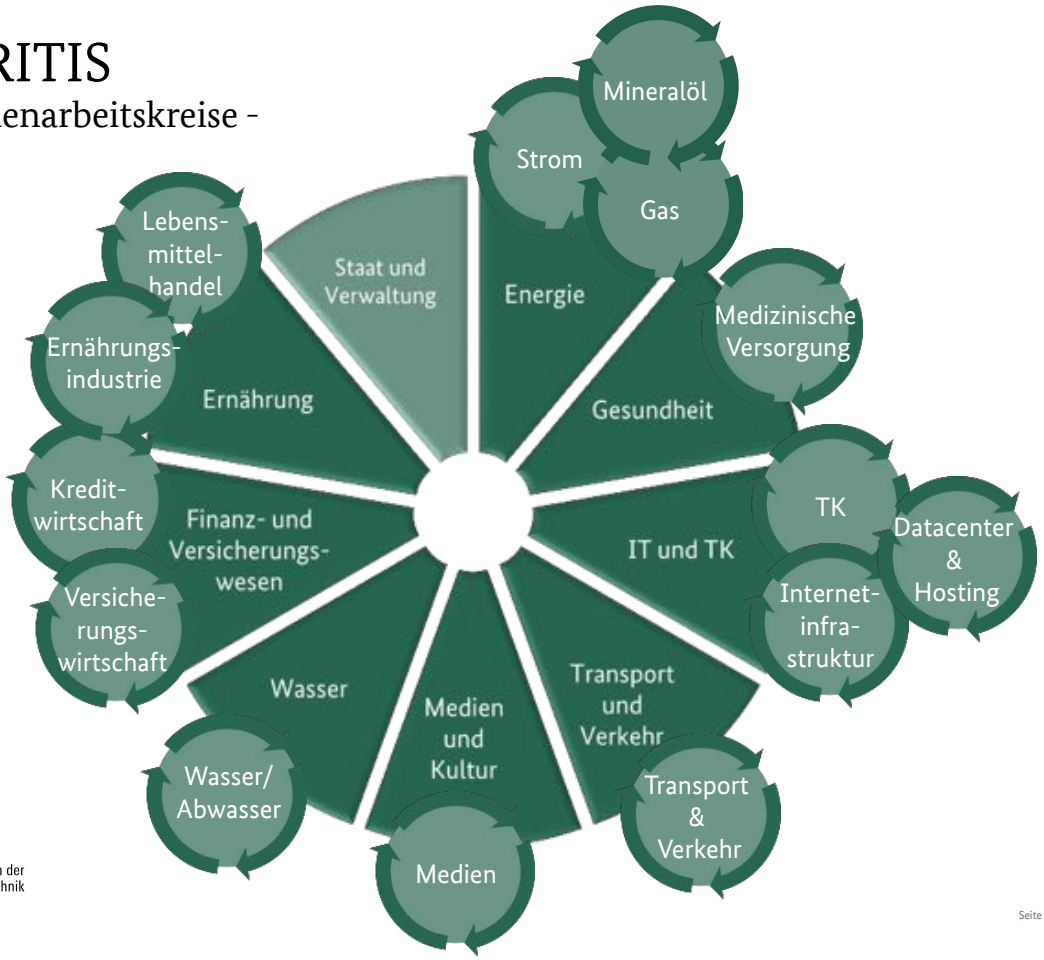
UP KRITIS

- Themenarbeitskreise -

- Anforderungen an Lieferanten
- Audits & Standards
- Industrial Control Systems (ICS)
- Internationales
- KRITIS-Tagung
- Operativer Informationsaustausch
- SPOC-Austausch
- Szenariobasierte Krisenvorsorge
- Transparenzpflichten
- Übungen

UP KRITIS

- Branchenarbeitskreise -



Branchenarbeitskreis Medien im UP KRITIS

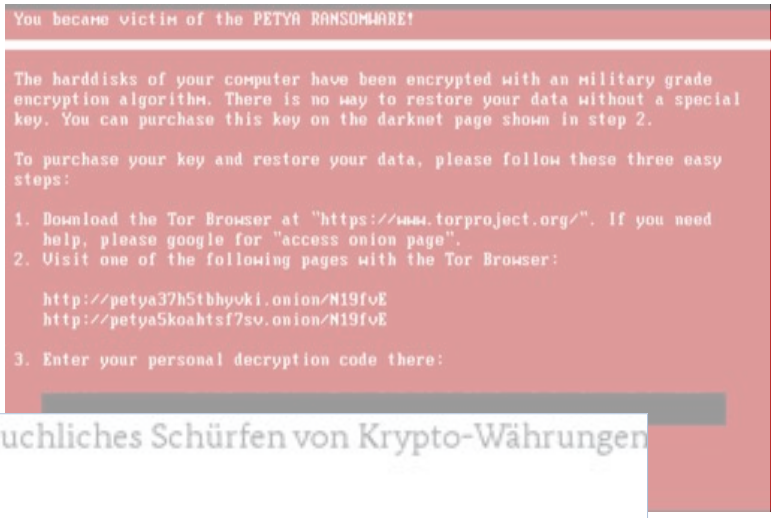
16 teilnehmende Organisationen aus dem Sektor

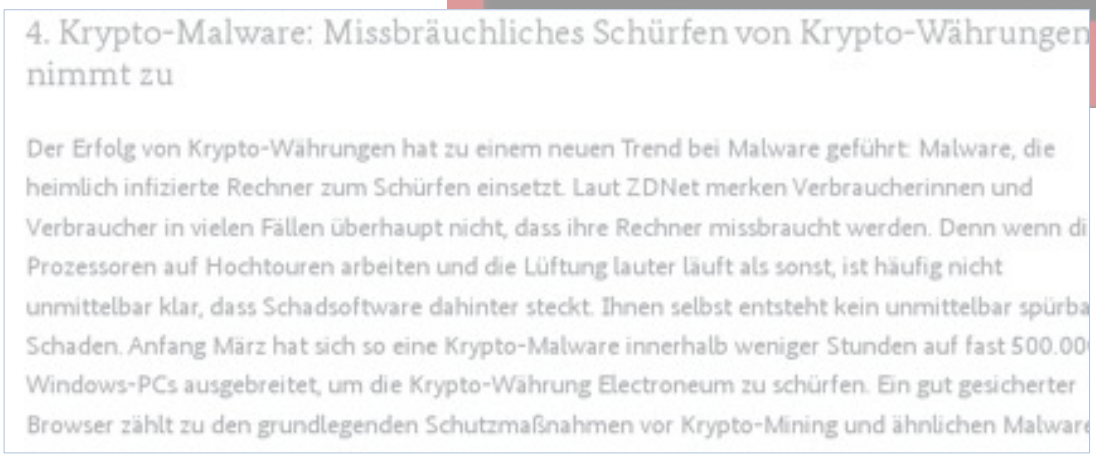
Aktuelle Themen:

- Freiwilliger Branchenstandard
- Security Level Agreement
- Operative Zusammenarbeit

Vorfälle

- Verschlüsselungstrojaner
- Mining Malware
- APT





4. Krypto-Malware: Missbräuchliches Schürfen von Krypto-Währungen nimmt zu

Der Erfolg von Krypto-Währungen hat zu einem neuen Trend bei Malware geführt: Malware, die heimlich infizierte Rechner zum Schürfen einsetzt. Laut ZDNet merken Verbraucherinnen und Verbraucher in vielen Fällen überhaupt nicht, dass ihre Rechner missbraucht werden. Denn wenn di Prozessoren auf Hochtouren arbeiten und die Lüftung lauter läuft als sonst, ist häufig nicht unmittelbar klar, dass Schadsoftware dahinter steckt. Ihnen selbst entsteht kein unmittelbar spürba Schaden. Anfang März hat sich so eine Krypto-Malware innerhalb weniger Stunden auf fast 500.00 Windows-PCs ausgebreitet, um die Krypto-Währung Electroneum zu schürfen. Ein gut gesicherter Browser zählt zu den grundlegenden Schutzmaßnahmen vor Krypto-Mining und ähnlichen Malware

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Dr. Uwe Jendricke
Bundesamt für Sicherheit in der Informationstechnik
Referat CK 32: Kritische Infrastrukturen – Grundsatz
Godesberger Allee 185-189
53175 Bonn

Tel. +49 (0) 228 99-9582 5507
Fax +49 (0) 228 99-10-9582-5507

uwe.jendricke@bsi.bund.de
www.bsi.bund.de
www.upkritis.de