



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

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/N19fvE>
<http://petya5koahstf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

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 die 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 spürbarer Schaden. Anfang März hat sich so eine Krypto-Malware innerhalb weniger Stunden auf fast 500.000 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

Prozesssteuerungen, spezielle und klassische IT



Prozesssteuerungssysteme (ICS)



Büro-IT



Spezialsysteme

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

Alte Betriebssysteme



Lösungswege



 **TLP WHITE // TLP AMBER**

 **CERT Bund**

Erste Hilfe bei einem APT-Angriff
Arbeitspapier - Version 3.0
22.01.2016
certbund@bsi.bund.de

BEST-PRACTICE-EMPFEHLUNGEN

für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen

EMPFEHLUNG: IT IN DER PRODUKTION

Industrial Control System Security

Top 10 Bedrohungen und Gegenmaßnahmen 2016

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln. Dies reicht von der Energieerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Fabrikautomation, Verkehrsleit-

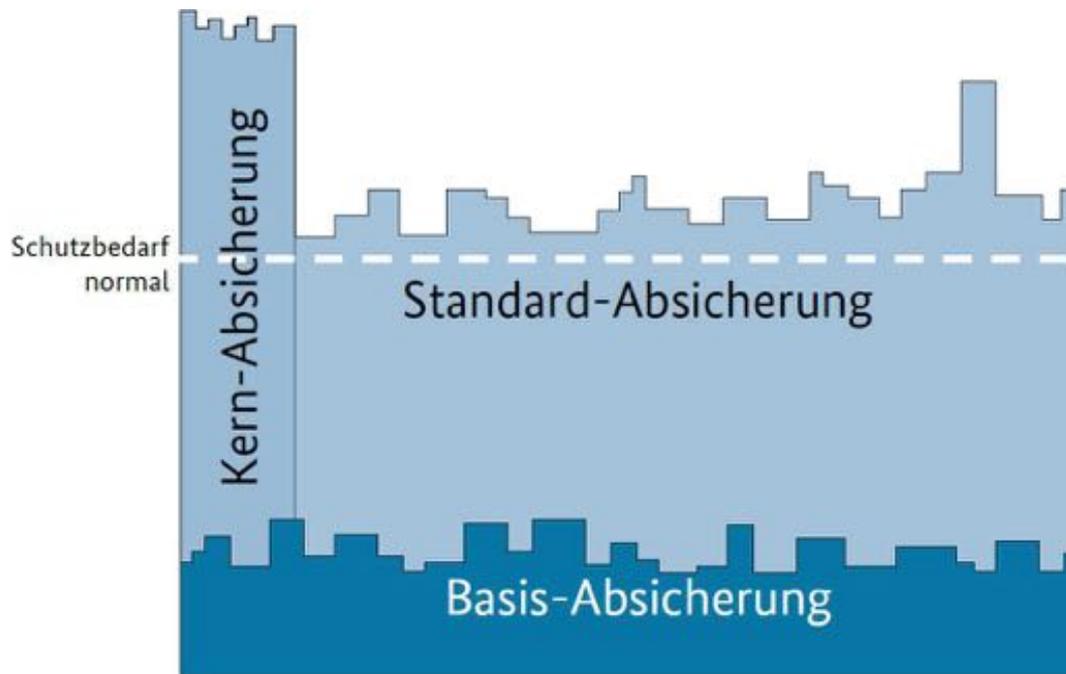
herheit

www.upkritis.de

<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

Bundesamt für Sicherheit in der Informationstechnik

Allianz für Cyber-Sicherheit

Informationspool Erfahrungsaustausch Angebote Meldestelle Über u...

Die Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Derzeit beteiligen sich nahezu 2350 teilnehmende Institutionen, über 83 aktive Partner und mehr als 45 Multiplikatoren an der Allianz.

Ziele und Angebote der Allianz für Cyber-Sicherheit

Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu...

- > Einführung
- Beirat
- Akteure
- Registrierung
- Liste der Teilnehmer
- Liste der Partner
- Liste der Multiplikatoren
- Kontakt

UP KRITIS

UP KRITIS
Öffentlich-Private Partnerschaft
zum Schutz Kritischer Infrastrukturen

- Grundlagen und Ziele -

www.upkritis.de

Kritische Infrastrukturen

- Sektoren -



UP KRITIS

- Vision -

*gemeinsame Verantwortung
von Staat und Wirtschaft*

*zentraler Beitrag zum Schutz
der Kritischen Infrastrukturen*

**UP KRITIS**

*Sicherstellung der Versorgung
der Bevölkerung*

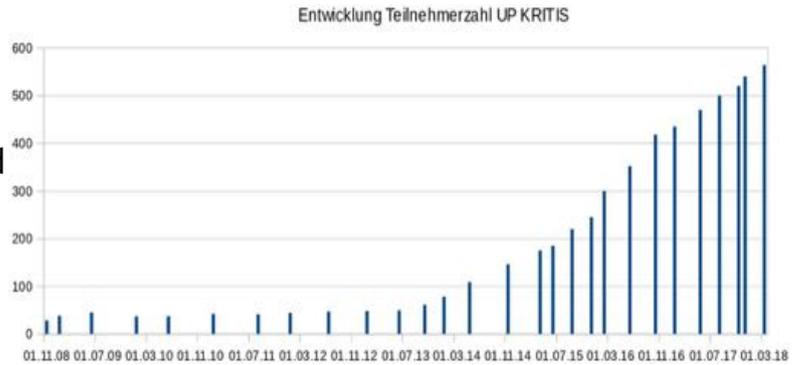
*Informationstechnik als
Schwerpunkt der Arbeiten*

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**



↑
Neues
Teilnehmer-
Modell

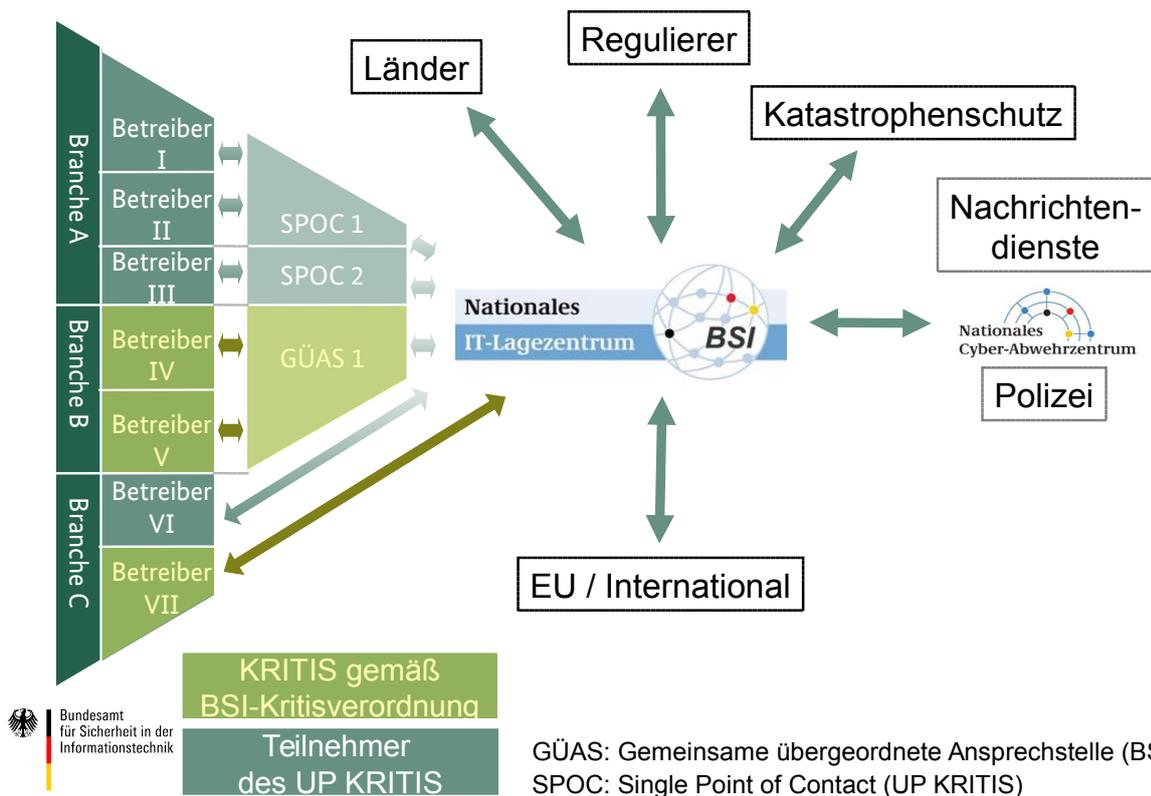
UP KRITIS

- Ziele -



UP KRITIS

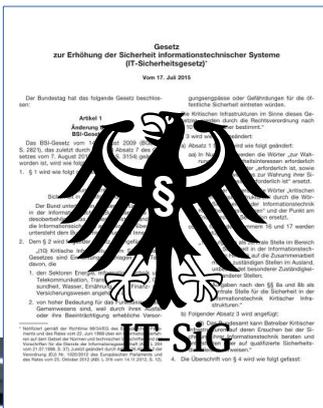
- Operativ: - Vernetzung, Informationsaustausch -



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

UP KRITIS

- Operativ: Meldewesen -



Bundesamt für Sicherheit in der Informationstechnik | Nationales IT-Lagezentrum | **BSI**

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kryptotrojaner 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 70 betroffene deutsche Unternehmen bekannt. Mit einer Vielzahl dieser Unternehmen wurde Kontakt...

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**

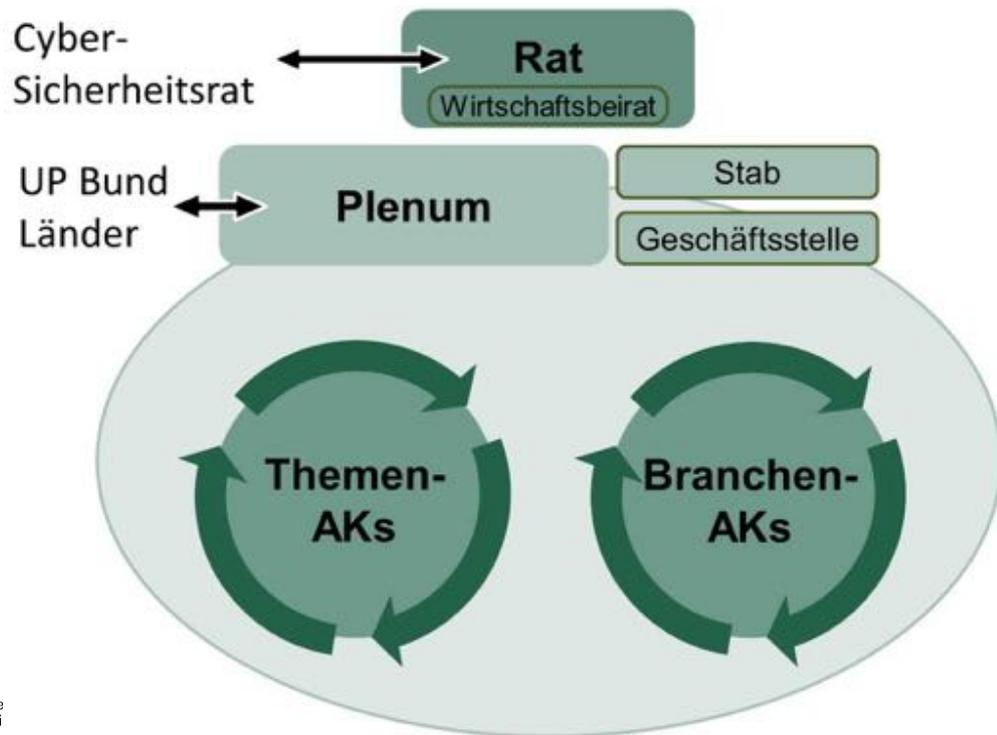
Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokuments und der darin enthaltenen Informationen gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

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 -



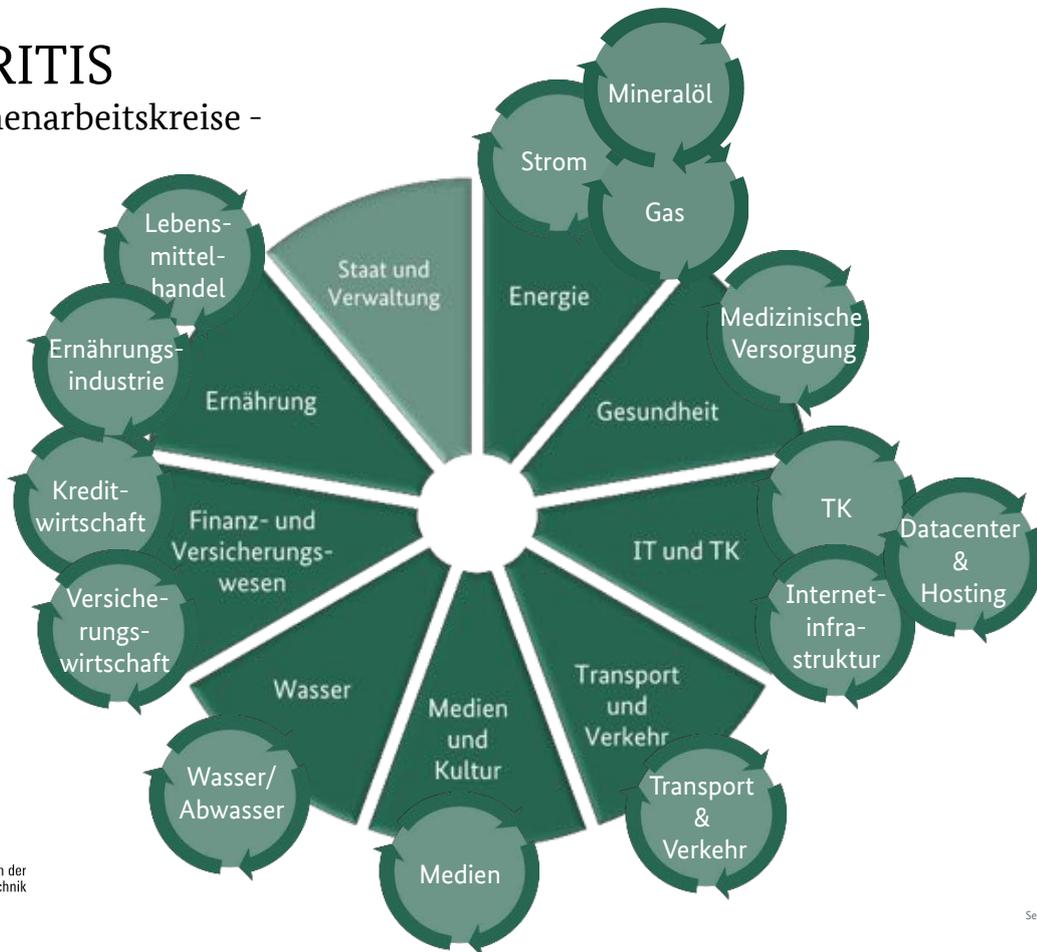
UP KRITIS

- Themenarbeitskreise -



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

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/N19fvE>
<http://petya5koahsf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

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 die 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 spürbarer Schaden. Anfang März hat sich so eine Krypto-Malware innerhalb weniger Stunden auf fast 500.000 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

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