Regulierung der Sicherheit im Cyberraum

ÜBERBLICK ÜBER WICHTIGE REGULATIVE MAßNAHMEN

DR. RAINER BAUMGART

Inhalt

- Situation der Cyber-Sicherheitslage
- Entwicklung der Regulierung der IT-Sicherheit
- Flankierende Regulierungen und Maßnahmen
- EU Aktivitäten
- IT Sicherheitsgesetz 2.0 (Entwurf)
- Ausblick

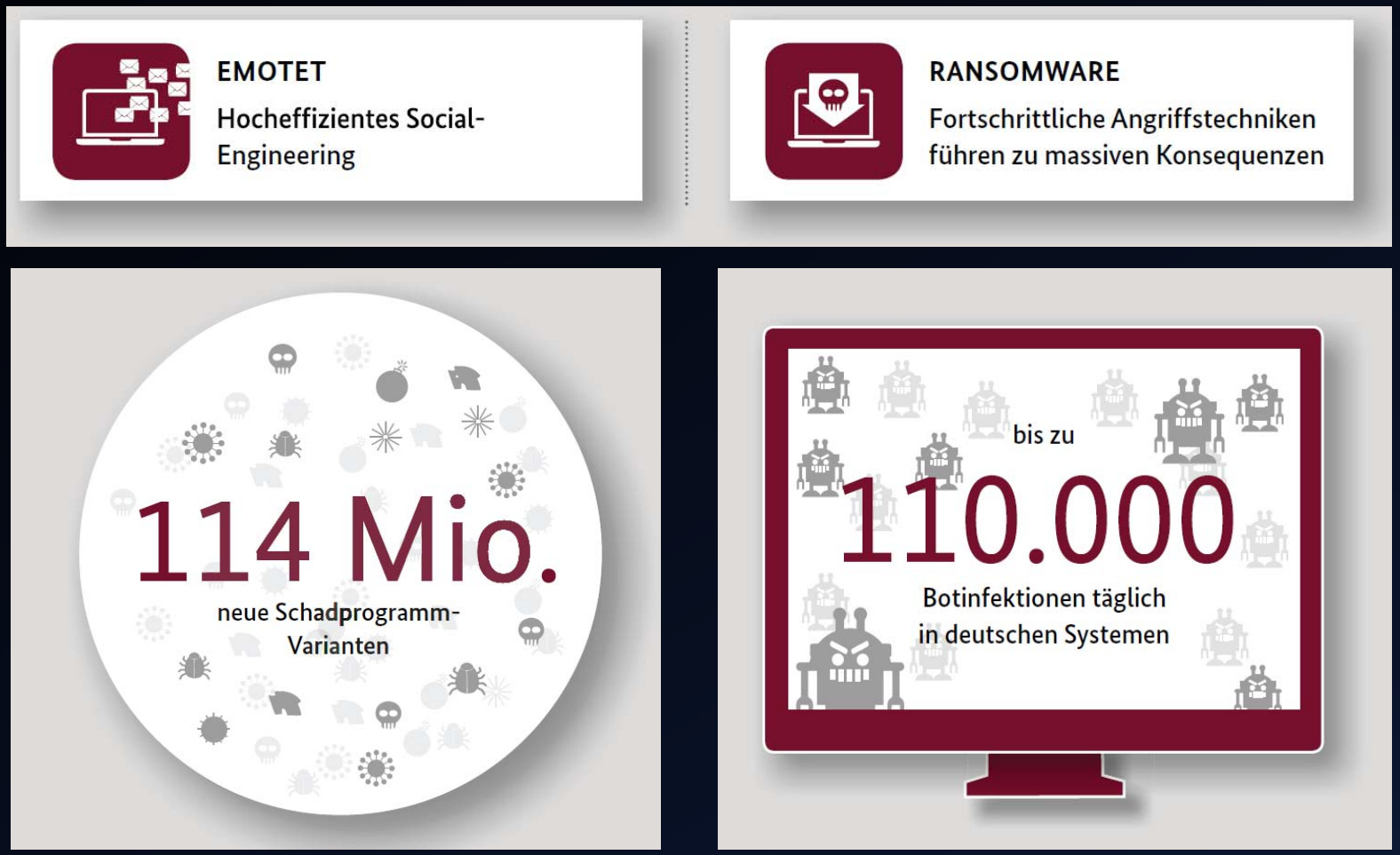
Situation

Zunehmende Bedrohung der (digitalen) Infrastrukturen

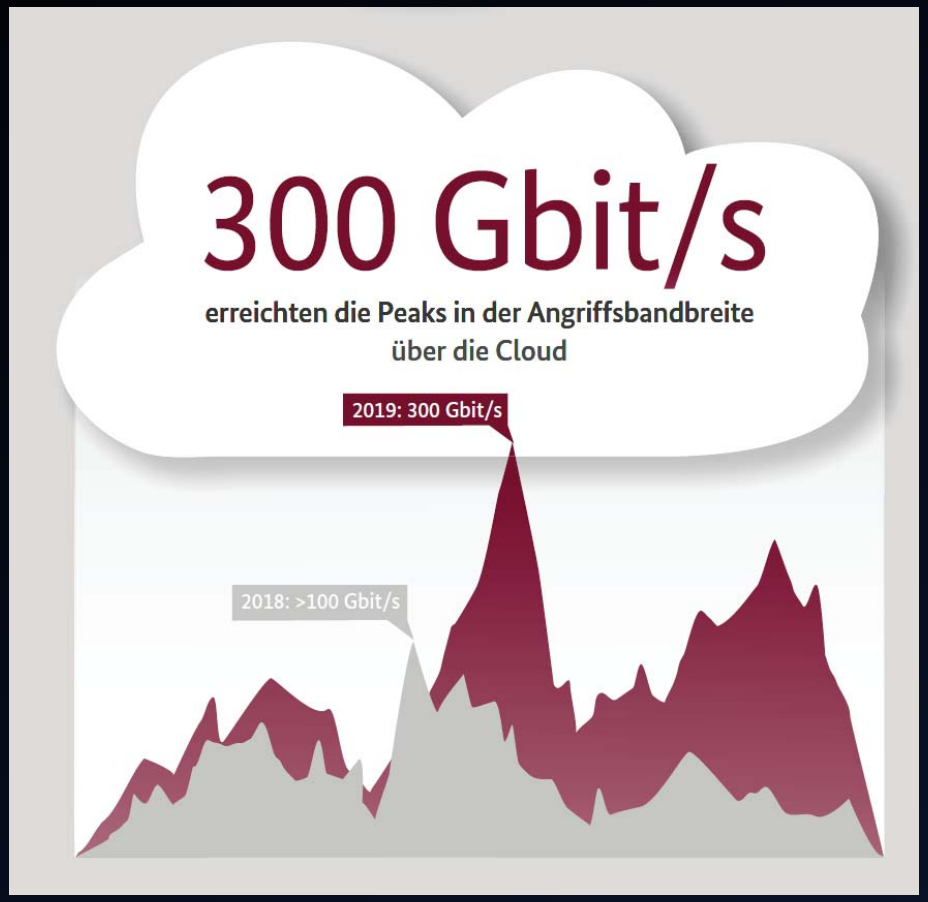
- Mittlerer Schaden eines Cyber-Angriffes für Unternehmen weltweit: Ø $3.86 million
- Geschätzte $20 billion Schäden durch Ransomware global
- 2020 werden ≈ 20.4 Mrd. IoT-devices existieren
- Nur ≈ 2% des IT Budgets geht in IT-Sicherheit

Cyber-Sicherheitslage 2019 in D

(BSI Report)

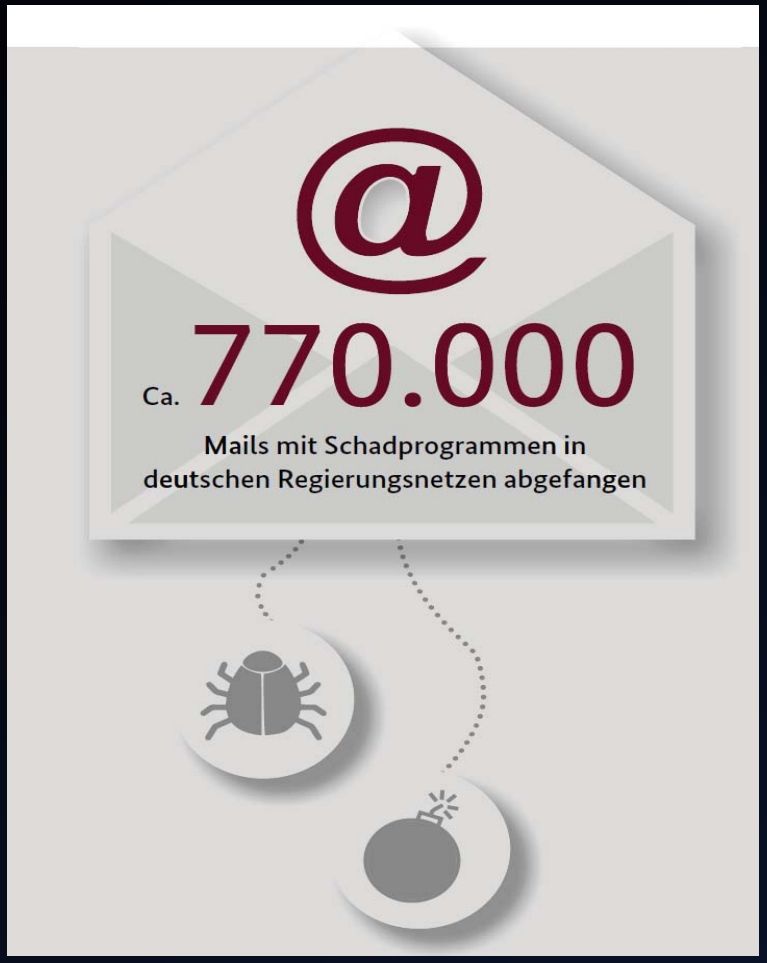


Cyber-Sicherheitslage 2019 in D
(BSI Report)



Cyber-Sicherheitslage 2019 in D

(BSI Report)



Inhalt

- Situation der Cyber Sicherheitslage
- Entwicklung der Regulierung der IT-Sicherheit
- Flankierende Regulierungen und Maßnahmen
- EU Aktivitäten
- IT Sicherheitsgesetz 2.0 (Entwurf)
- Ausblick

BSI Gesetz

BSI = Bundesamt für Sicherheit in der Informationstechnik
Erstfassung 1991 (Errichtungsgesetz)
Neufassung 2009

- Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes
- Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen
- Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen

BSI Gesetz II

- Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen
- Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen
- Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes

BSI

Zentrale Rolle im IT-Sicherheitsgesetz seit 2015 zugewiesen

- Zentrale Meldestelle für die Sicherheit in der Informationstechnik
- Warnungen
- Besondere Anforderungen an Anbieter digitaler Dienste
- Zertifizierung
- Ermächtigung zum Erlass von Rechtsverordnungen
- Bußgeldvorschriften

IT Sicherheitsgesetz

Erste Version 2015 verabschiedet

- Ändert und ergänzt Energiewirtschaftsgesetz, Telemediengesetz, Telekommunikationsgesetz und weitere Gesetze
- Betreiber kritischer Infrastrukturen müssen IT-Sicherheit nach dem "Stand der Technik" umsetzen und deren Einhaltung regelmäßig gegenüber dem BSI nachweisen
- Betreiber müssen dem BSI erhebliche Störungen ihrer IT melden
- BSI erhält Befugnis IT-Produkte auf ihre Sicherheit hin zu untersuchen

IT Sicherheitsgesetz

- Möglichkeit des Bundesinnenministeriums, Mindeststandards vom BSI für alle Behörden als verbindlich zu erklären
- Jährlicher Lagebericht informiert die Öffentlichkeit über die aktuellen Gefahren
- Änderung Telekommunikationsgesetz:
  - "Stand der Technik" nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur einzusetzen und zu erhalten (Aufsicht Bundesnetzagentur)

IT Sicherheitsgesetz

- Erster Teil BSI Kritis Verordnung 2016:
  - Betroffene Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung
- Änderung der BSI-Kritis Verordnung 2017:
  - Ergänzt um die Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr

IT Sicherheitsgesetz
BSI Kritisverordnung

- Betroffene Organisationen haben:
  - eine Kontaktstelle zu benennen
  - IT-Störungen zu melden
  - den "Stand der Technik" umzusetzen
  - dies alle zwei Jahre gegenüber dem BSI nachzuweisen

- Auch Partner, Dienstleister und Lieferanten der identifizierten Organisationen müssen dem nachkommen

Inhalt

- Situation der Cyber Sicherheitslage
- Entwicklung der Regulierung der IT-Sicherheit
- Flankierende Regulierungen und Maßnahmen
- EU Aktivitäten
- IT Sicherheitsgesetz 2.0 (Entwurf)
- Ausblick

EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Directive)

Von 7.2016 – 2 Jahre Zeit zur nationalen Umsetzung

April 2017 hat der Bundestag das neue NIS-RL-Umsetzungsgesetz verabschiedet

- Anpassung der Aufsichtsbefugnisse des BSI
- Regelungen zu MIRTs (Mobile Incident Response Teams)
- Regelung von Berichtspflichten und Pflichten zur Konsultation anderer Mitgliedstaaten bei grenzüberschreitendem Bezug
- Konkretisierungen der Meldepflichten der Betreiber
- Einführung von Mindestanforderungen und Meldepflichten
- Aufsichtsbefugnisse und Sanktionen für die in der NIS-RL konkret genannten digitalen (Telemedien-) Dienste

Inhalt

- Situation der Cyber-Sicherheitslage
- Entwicklung der Regulierung der IT-Sicherheit
- Flankierende Regulierungen und Maßnahmen
- EU Aktivitäten
- IT Sicherheitsgesetz 2.0 (Entwurf)
- Ausblick

IT-Sicherheitsgesetz 2.0

liegt seit 4.2019 als Referentenentwurf vor

Entwurf beinhaltet u.a.:

- Erweiterung der Sektoren um produzierende Großindustrie sowie Chemieindustrie und Abfallentsorgung
- Hersteller von IT-Produkten sollen verstärkte Meldepflicht gegenüber dem BSI haben, wenn KRITIS-Anlagen betroffen sind
- Meldepflichten für Hersteller von KRITIS-Kernkomponenten

IT-Sicherheitsgesetz 2.0

Entwurf beinhaltet u.a.:

- Freiwilliges IT-Sicherheitskennzeichen (Herstellererklärung)
- Verschärfung der Bußgeldregelungen
- Straftatbestand für das Betreiben illegaler Darknet-Handelsplätze
- Zugangsanbieter können verpflichtet werden schädlichen Datenverkehr zu blockieren

1.500
registrierte KRITIS-Anlagen

2019:
252
Meldungen von KRITIS-Betreibern

2018:
145
Meldungen von KRITIS-Betreibern

Inhalt

- Situation der Cyber-Sicherheitslage
- Entwicklung der Regulierung der IT-Sicherheit
- Flankierende Regulierungen und Maßnahmen
- EU Aktivitäten
- IT Sicherheitsgesetz 2.0 (Entwurf)
- Ausblick

Kritik (Auszüge und Beispiele)

- Unbestimmtheit der im Gesetzentwurf enthaltenen Begrifflichkeiten "Berücksichtigung des Standes der Technik" und "erheblicher Sicherheitsvorfall"
- Unabhängigkeit des BSI (Staatstrojaner ↔ Abwehrmaßnahmen) (CCC)
- Nachträgliche Einstufung zur "kritischen Infrastruktur" durch Rechtsverordnung widerspricht Art. 80 des Grundgesetzes (Roßnagel)
- KRITIS-Betreiber alleine oft nicht in der Lage ein Software-Update bei Sicherheitslücken zu generieren

Die Spirale der Regulierung der Cyber(un)sicherheit

Ausblick

- Zunehmende Bürokratisierung
- Zunehmender formaler Aufwand für Betreiber bei gleichzeitig steigender Bedrohungslage
- Zunehmender Aufbau der Verwaltungsstrukturen bei BSI, BKA, etc.
- Zunehmende Aktivitäten der EU mit nationalen Auswirkungen
- Zunehmende Abhängigkeit der Betreiber von Beratern und Fachpersonal
- Zunehmender Bedarf an Zertifizierungen von Sicherheitsprodukten
- Zunehmender Verlust der „Digitalen Souveränität“

Vielen Dank für Ihre Aufmerksamkeit