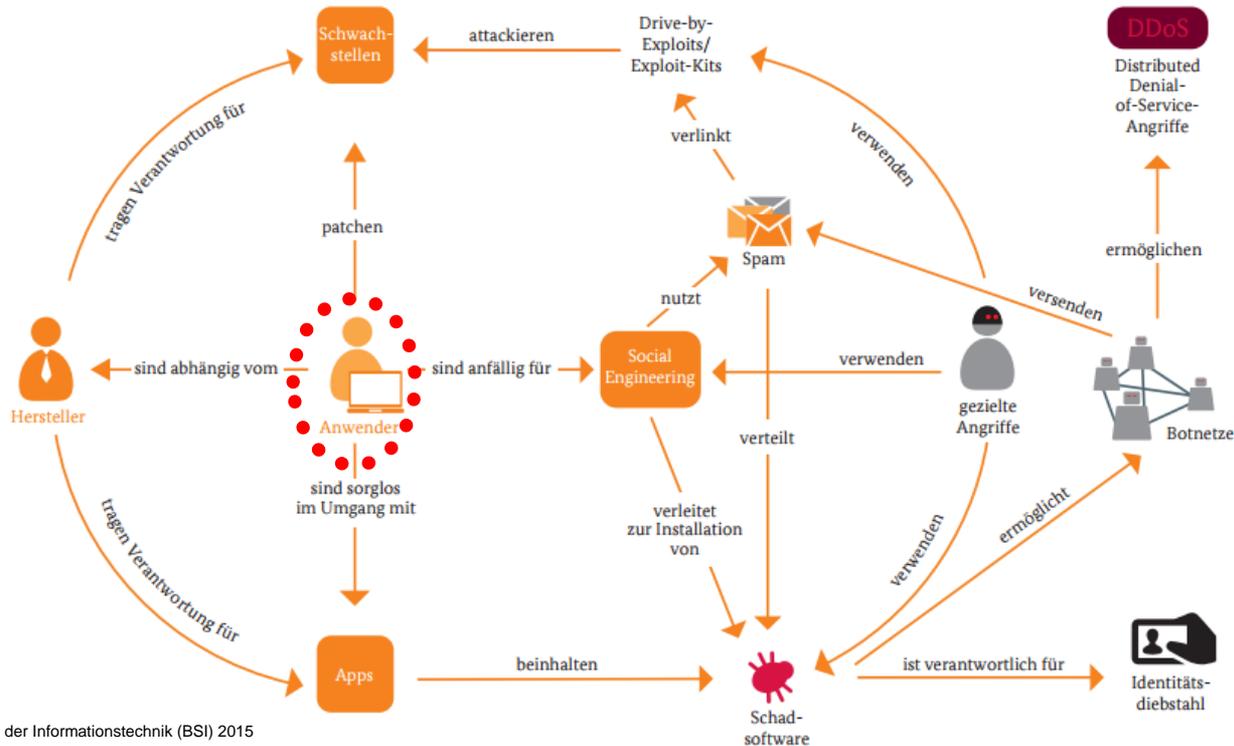


Informationsveranstaltung  
„Spionage – (k)ein Thema“  
am 26.01.2016  
in Hannover

# Cyberangriffe – Auswirkungen auf deutsche Behörden und staatliche Institutionen



# Ursachen für Cyberangriffe



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) 2015

# Rahmenbedingungen

- Cloud, Mobile, Social Media, Big Data
- Digitalisierung von Gesellschaft u. Industrie (4.0)
- Cyberkriminalität, Underground Economy
- Spionage, Wirtschaftsspionage
- Internet der Dinge, SCADA-Steuerungssysteme
- Bedrohung Kritischer Infrastrukturen
- Cyberterrorismus
- Cyberwar

# Rahmenbedingungen

Können wir uns schützen?

# Aktivitäten auf EU-Ebene

- Entwurf Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (COM 2013/48 final - NIS-Richtlinie)
- Entwurf der Cybersicherheitsstrategie der EU (JOIN(2013) 1 final)
- EC3: Europäisches Zentrum zur Bekämpfung der Cyberkriminalität bei Europol



# Aktivitäten des Bundes

- 2011: nationale Cybersicherheitsstrategie
- 2011: nationaler Cybersicherheitsrat (Bund + zwei Ländervertreter),

nationales Cyberabwehrzentrum des Bundes (beim BSI) - Prävention, Information und Frühwarnung gegen Cyber-Angriffe



- 2013: Koalitionsvertrag: IT-Sicherheitsgesetzes, europäische Cybersicherheitsstrategie
- 2015: IT-Sicherheitsgesetz



# Aktivitäten des Bundes

- Allianz für Cybersicherheit
  - BSI und BITKOM
  
- Umsetzungsplan KRITIS
  - öPPP zum Schutz von KRITIS
  
- Digitale Agenda 2014 - 2017



# Aktivitäten der Länder

- Innenministerkonferenz:  
Einrichtung einer länderoffenen  
Arbeitsgruppe Cyber-Sicherheit auf StS-Ebene
- IT-Planungsrat Bund/Länder:  
Verabschiedung einer Informationssicherheitsleitlinie  
Arbeitsgruppe Informationssicherheit
- Gemeinsames Arbeitsprogramm
  - Verwaltungs-CERT-Verbund
  - Aufbau ISMS
  - Rechtsgrundlagen IDP/IDS/SIEM
  - Hilfestellung f. Kommunen
  - Krisenübungen
  - Industrie 4.0 und Datenschutz



# Cybersicherheit entsteht durch



- Gefahrenabwehr
- Kriminalitätsbekämpfung und
- vorausschauenden Katastrophenschutz
- bessere Informationssicherheit innerhalb und außerhalb der öffentlichen Verwaltung,



# Technische Vernetzung

- Sensorik – Detection
  - Interne und externe Sensorik
  - Automatisierte Auswertung, SIEM
- Intelligence Feeds
- Threat Clouds



# Vernetzung innerhalb der Verwaltung

- Polizei / LKA, Verfassungsschutz / Wirtschaftsschutz / Landes-CERT
  - Austausch von Angriffsvektoren
  - Austausch von Indikatoren von Schad- und Spionagesoftware
  - Austausch von Metainformationen über aktuelle Sicherheitsvorfälle
  - Austausch von Handlungsempfehlungen

## Vernetzung auf der Ebene Bund + Länder

- Verwaltungs-CERT-Verbund (VCV)
- Länderübergreifende Arbeitsgruppen
  - Austausch von Angriffsvektoren
  - Austausch von Indikatoren von Angriffen
  - Austausch von Konzepten, Strategien, Erfahrungen
  - Gemeinsames Nutzen von Ressourcen
  - Frühwarninformationen

# Vernetzung mit Wirtschaft und Forschung

- Allianz für CyberSicherheit (ACS)
- Deutscher CERT-Verbund (DCV)
  - Austausch von Angriffsvektoren
  - Austausch von Indikatoren auf Schadsoftware
  - Austausch von Strategien und Erfahrungen
  - Gemeinsames Nutzen von Ressourcen
  - Frühwarninformationen
  - Lagebilder



**CERT-Verbünde**  
(Verwaltungs-CERT-  
Verbund, Deutscher CERT-  
Verbund)

**Sicherheits-  
organisationen**  
(LKA, Verfassungsschutz,  
Wirtschaftsschutz, BSI)



**Eigene Quellen**  
(IDS, SIEM)



**Öffentliche Quellen**  
(Fachpresse, Portale)

**Niedersächsische  
Kommunal-  
verwaltung**

**Niedersächsische  
Landesverwaltung**  
(Ressorts, nachgeordnete  
Dienststellen und  
landesinterne IT-  
Dienstleister)

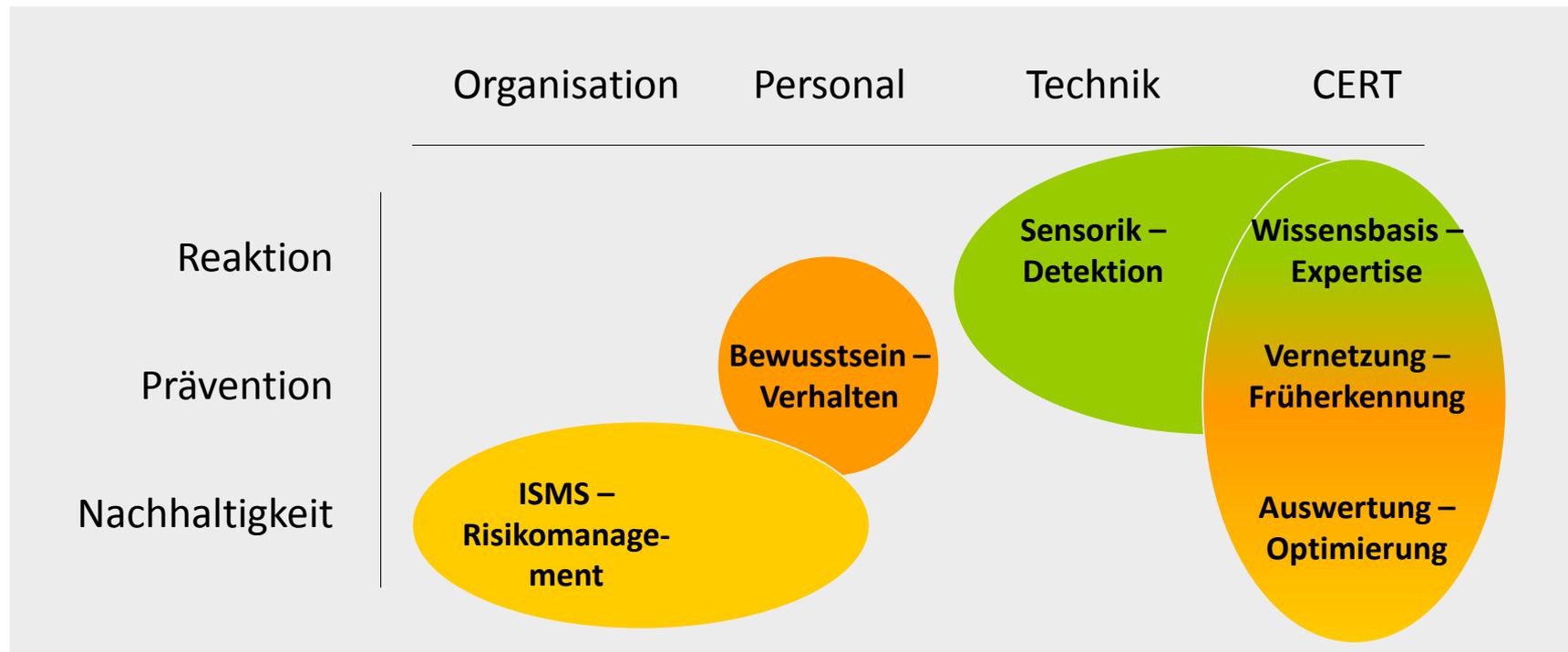


## Ergebnis der Vernetzung

- Generieren der Informationssicherheitslage aus externen und internen Informationen
- Generieren von Infrastrukturspezifischen Handlungsempfehlungen
- Früherkennung von Sicherheitslücken und zielgerichteten Cyberangriffen
- Effektive Verteidigungsstrategien



# Verteidigungsstrategien...



# Verteidigungsstrategien...

Können wir uns schützen?

# Verteidigungsstrategien...

Ja!

# Kontakt

**Niedersachsen-CERT**  
cert@niedersachsen.de  
0511 - 120 - 4798



## Informationssicherheit in Niedersachsen

März 2014

### INFORMATIONSSICHERHEITSTRATEGIE

Informationssicherheit als übergreifender Prozess für die gesamte Niedersächsische Landesverwaltung.

**INKLUSIVE  
LEITLINIE UND  
ALLER BISHER  
IN KRAFT  
GETRETENEN  
RICHTLINIEN**



### SICHERHEITSKONZEPTION FÜR LANDESBEHÖRDEN

Ein praxisorientiertes Vorgehensmodell für die Erreichung von Sicherheitskonzeptionen auf Basis einer Risikoanalyse.

