Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-Sicherheit

Maßnahmen und Kooperationen

Marc Schober
BSI

Referat C23 - „Allianz für Cyber-Sicherheit, Penetrationszentrum und IS-Revision“

egov-day, Koblenz / 13.06.2013

Zahlen und Fakten

in 2012 mehr als **5.000** neue Schwachstellen in Standardsoftware

etwa alle **2 Sekunden** ein neues Schadprogramm oder eine Variante

pro Minute **2 gestohlene digitale Identitäten** in Deutschland

pro Monat etwa **40.000** blockierte Zugriffsversuche auf schädliche Websites aus dem Regierungsnetz

Ursachen für Cyber-Probleme

- Schwachstellen in Standardprodukten
- Ungepatchte Systeme (Bürger / KMU, …)
- Industrielle Fertigung von Malware
  - Malware Construction Kits
- Cyber-Angreifer
  - Hacktivisten, professionelle Cyber-Kriminelle, Wirtschaftsspione, ND, ...
  - Zukünftig Cyber-Terroristen und Cyber-War-Staaten?
- Cyber-Täter im Hintergrund
  - Entwickler von Exploit-Kits, Botnetz-Betreiber, DDoS-Angriffs-Dienstleister,...

Bundesamt
für Sicherheit in der
Informationstechnik

Ungezielte Cyber-Angriffe in der Fläche

- **Angriffsvektor E-Mail**
  - Verteilung von Malware im Anhang von SPAM-Mails
- **Angriffsvektor Drive-By-Exploits**
  - Verteilung von Malware mittels manipulierter Webseiten z.B. über manipulierte Werbebanner

Auswirkungen

- Botnetze als Folge ungezielter Cyber-Angriffe
  - Trend → zunehmend Botnetze aus gekaperten Servern = höhere Leitungskapazitäten für DDoS-Angriffe!
- Eigenes System unter fremder Kontrolle
  - Diebstahl digitaler Identitäten (> 1.100.000 belegte Fälle in 2012)
  - Diebstahl von Geldwerten

Gezielte Cyber-Angriffe
Sabotage

- **Distributed Denial of Service – Angriffe (DDoS)**
  - DNS-Server (2012)
  - US-Banken (seit 2012), Niederländische/Belgische Banken (2013)
  - Spamhaus (2013)

- **Hacking / Malware**
  - Stuxnet → Urananreicherungsanlage im Iran (2010)
  - NH-Bank in Südkorea (2011)
  - Saudi-Aramco (2012)

Trend → Kombinierte Angriffe

- Sabotage-Angriffe (DDoS) zur Ablenkung, dann gezielte Spionage-Angriffe

Gezielte Cyber-Angriffe
Spionage

- Die wenigsten Fälle sind öffentlich bekannt
- Sowohl Großunternehmen als auch KMU betroffen
- Die wenigsten Fälle kommen zur Anzeige
- Die meisten Cyber-Spionage-Fälle werden nur zufällig erkannt

Mehrstufige Angriffe

→ Angriffe auf Sicherheitsinfrastrukturen zur Vorbereitung des Angriffs auf ein anderes Ziel

- DigiNotar (2011)

Maßnahmen
1. Eigenverantwortung

Grundsätzlich:
Eigenverantwortung der Betreiber von IT-Systemen zu deren Schutz

IT-Sicherheit ist Managementaufgabe!

Unterstützung der Umsetzung u.a. durch:

- IT-Sicherheitsstandards (IT-Grundschutz, …)

- Sichere Produkte
- Qualifizierte Dienstleister

→ ggf. Nachweis durch Zertifizierung

Maßnahmen
2. Staatliche Maßnahmen

- Cyber-Sicherheitsstrategie für Deutschland (2011)
  - u.a.: Schutz Kritischer Informationsinfrastrukturen,
  - Sichere IT-Systeme in Deutschland,
  - Stärkung der IT-Sicherheit in der öffentlichen Verwaltung, ...

- BSI IT-Lagezentrum & CERT-Bund
  - Beobachten, Beurteilen, Bewältigen
  - Zusammenarbeit mit vielen Akteuren über versch. Initiativen (CERTs, Bund, Länder, Wirtschaft)
- IT-Krisenreaktionszentrum
- Cyber-Abwehrzentrum

- **und zahlreiche weitere Initiativen und Maßnahmen**

Maßnahmen
3. Kooperation

Gegenseitiger Austausch von Informationen und Erfahrungen ist einer der wichtigsten Bausteine der IT-Sicherheit

Kooperation zwischen ...

- staatlichen Stellen
  - unterschiedlichste Ebenen z.B. European Governmental CERT Group (EGC)
  - Bund-Länder z.B. VerwaltungsCERT-Verbund
- innerhalb der Wirtschaft z.B. unter IT-Security-Professionals
- Staat, Wirtschaft und andere Institutionen
  - im Bereich der Kritischen Infrastrukturen → UP KRITIS
  - Zwischen CERTs → z.B. CERT-Verbund zwischen den Deutschen CERTs
  - allgemein → z.B. Allianz für Cyber-Sicherheit


Allianz für
Cyber-Sicherheit

Allianz für Cyber-Sicherheit

Die Allianz ist

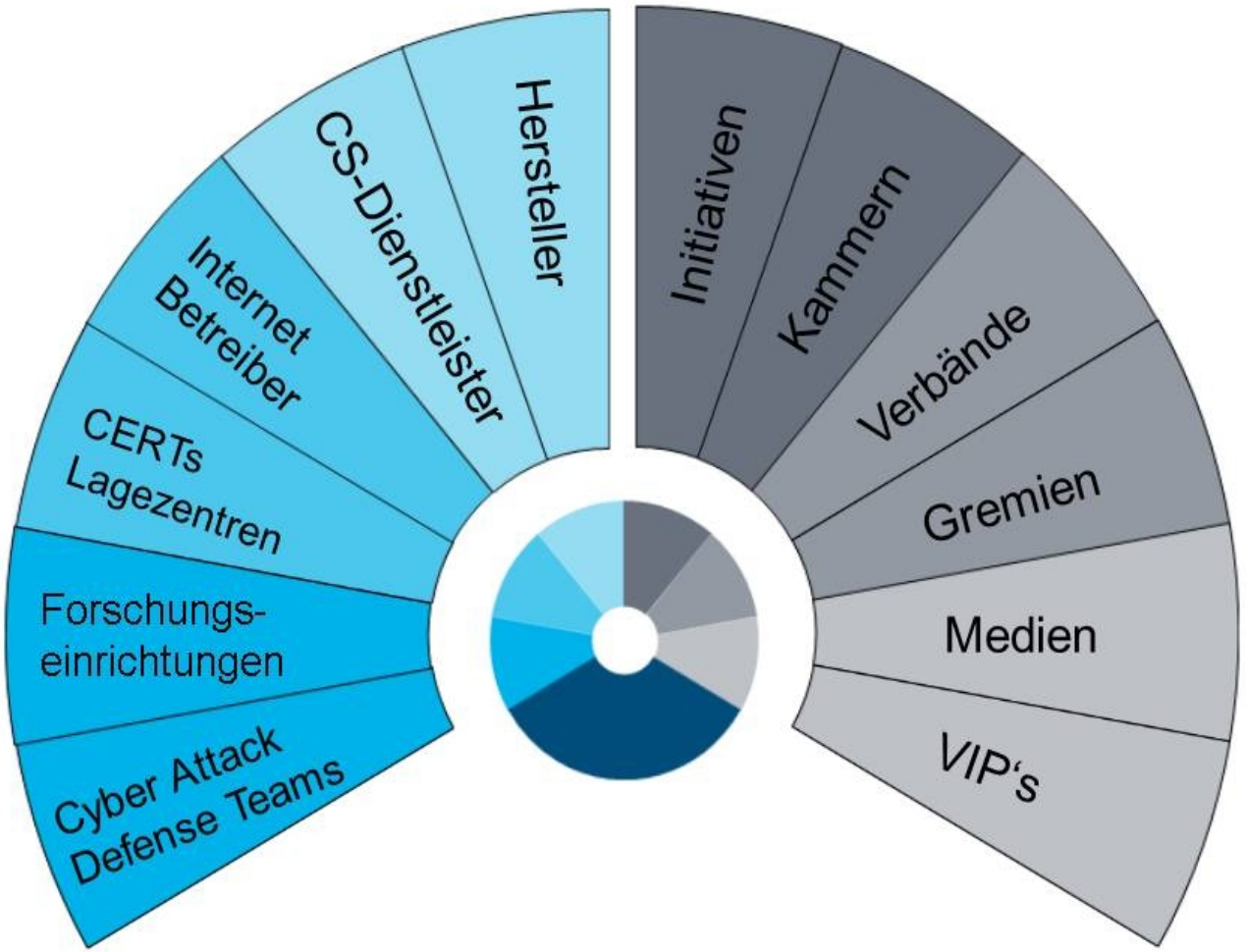
- kein politisches Gremium, sondern praktische Hilfe
- von Profis für Profis
- neutral

In Zahlen

- 78 Partner
- 24 Multiplikatoren
- mehr als 220 teilnehmende Institutionen
- 3 Experten-/Arbeitskreise, 6 + **X** jährliche Veranstaltungen

Allianz für Cyber-Sicherheit
Zielgruppen

Allianz für Cyber-Sicherheit
Partner und Multiplikatoren



Was bietet die Allianz für Cyber-Sicherheit?

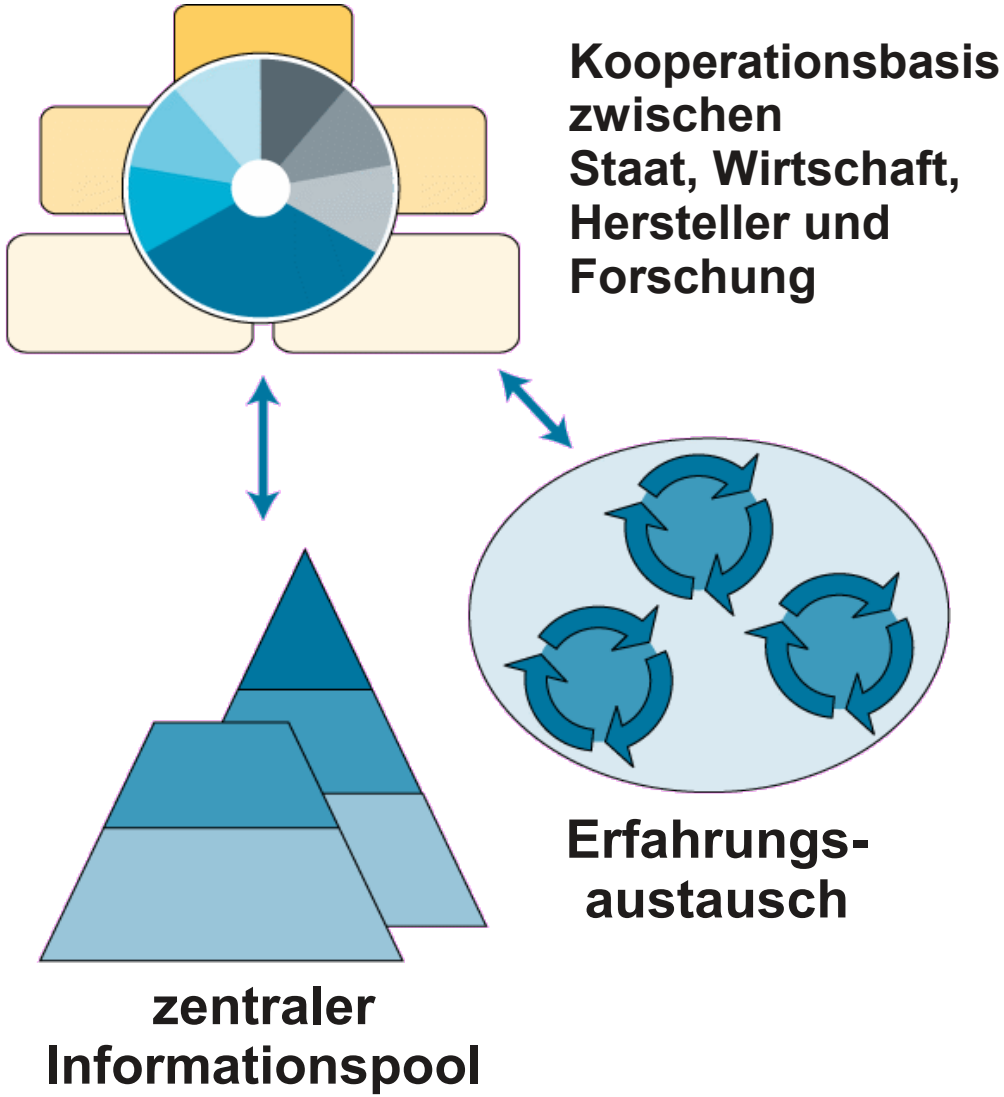
Informationspool

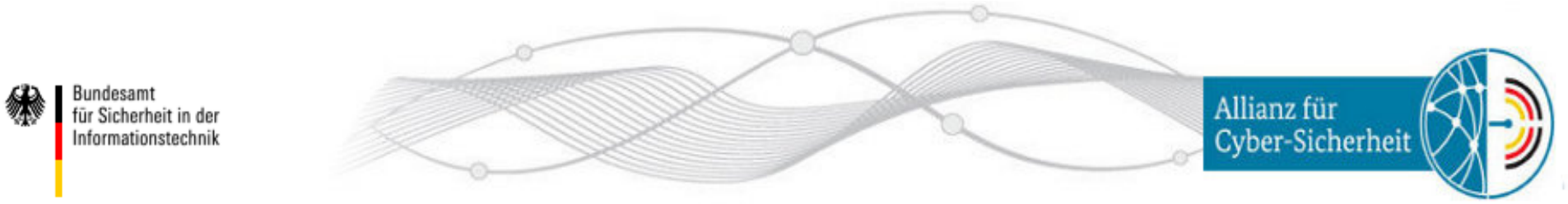
- Cyber-Sicherheitslage, Warnmeldungen, ...
- Analysen, Empfehlungen, Hintergrundinfos, ...

Abgestuft in öffentl., nicht-öffentl. und vertrauliche Informationen

Erfahrungsaustausch

- Partner- / Teilnehmertage
- Experten- / Arbeitskreise
- Regionale Erfa-Kreise
- ...





Sie sind hier:> Startseite > Offener Bereich > Dokumente

Dokumente

- Sensibilisierung
- Sofortmaßnahmen
- Cyber-Sicherheitslage
- Angriffsmethoden
- Werkzeuge
- Zert. Dienstleister
- Analysen
- Empfehlungen
- BCM

Allianz für Cyber-Sicherheit

In diesem Bereich stehen Ihnen öffentliche Informationen der Allianz für Cyber-Sicherheit zur Verfügung. Hier finden Sie unter anderem Dokumente des BSI, Beiträge der Partner wie auch Termine und Veranstaltungen. Wenn Sie allgemeine Informationen zur Allianz für Cyber-Sicherheit oder zum Registrierungsprozess benötigen, finden Sie diese unter dem Menüpunkt "→ Allgemeine Informationen".

Aktuelle Dokumente

Die folgenden 5 Dokumente wurden zuletzt eingestellt oder geändert:

- Sichere Nutzung von PCs unter Microsoft Windows 7 - für kleine Unternehmen und Selbstständige v1.3 (27.02.2013)
- Soziale Medien & soziale Netzwerke - Einsatz im Unternehmenskontext v1.0 (14.02.2013)
- Bereitstellung von Webangeboten v1.0 (05.02.2013)
- Handhabung von Schwachstellen v1.1 (31.01.2013)
- TLS/SSL Best-Practice v1.1 (16.01.2013)

Aktuelle Dokumente von Partnern

Bitte beachten Sie, dass die Partnerbeiträge größtenteils auf den Webseiten der Partner angeboten werden. Daher kann es vorkommen, dass Sie die Webpräsenz der Allianz für Cyber-Sicherheit verlassen, wenn Sie auf einen Beitrag klicken.

www.allianz-fuer-cybersicherheit.de

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Marc Schober
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5929
Fax: +49 (0)22899-10-9582-5929

marc.schober@bsi.bund.de

www.bsi.bund.de
www.allianz-fuer-cybersicherheit.de