Bundesamt
für Sicherheit in der
Informationstechnik

Herausforderungen der Informationssicherheit im Zeitalter der Digitalisierung – das BSI als Partner der Bundeswehr

Arne Schönbohm, Präsident

01. September 2016
Koblenzer IT-Tagung

1. Ausgangssituation

Kennzeichen der Digitalisierung

Die Digitalisierung prägen *drei zentrale Charakteristika*, aus denen sich die Herausforderungen für die Informations- und Krypto-Sicherheit ergeben:

- *Technologische Durchdringung und Vernetzung*
- *Komplexität*
- *Allgegenwärtigkeit*

Kennzeichen der Digitalisierung

Informationstechnik heute

Technologische Durchdringung und Vernetzung:
Alle physische Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden .

Komplexität:
Die Komplexität der IT nimmt durch vertikale und horizontale Integra-tion in die Wertschöpfungsprozesse erheblich zu.

Allgegenwärtigkeit:
Jedes System und jede Information ist praktisch zu jeder Zeit und von jedem Ort über das Internet für unterschiedlichste Plattformen für jedermann erreichbar .

Gefährdungslage:
Wandel der Bedrohungslage - Herausforderung für alle

- *Cyber-Angriffe – (beinahe) ein Alltagsphänomen? !*

  Cyber-Angriffe auf
  - Bundeswehr und Behörden
  - Unternehmen
  - Privatnutzer

  kommen jeden Tag vor.
- Cyber-Angriffe haben die Phase einer *ernsthaften Bedrohung und Gefährdung* unserer öffentliche Verwaltung, Wirtschaft und Gesellschaft erreicht.
- Dies gilt auch für die *Bundeswehr.*

Gefährdungslage:
Wandel der Bedrohungslage - Herausforderung für alle

- Cyber-Angriffe sind *komplexer* und *mehrdimensionaler* (Kombination und Vielfältigkeit der unterschiedlichen Angriffsvektoren) geworden.
- *Angreifer werden professioneller*
- *Änderung von Rahmenbedingungen führen zu verstärkter Asymmetrie zwischen Angriff und Verteidigung zum Vorteil der Angreifer:*
  - neue technologische Angriffsmöglichkeiten
  - zunehmende Komplexität der Technologie
  - Unbedarftheit der Nutzer
  - Überforderung der Nutzer

2. Auswirkungen der Cybergefährdungen

Wie bedroht ist Deutschlands Cyber-Raum?

Täglich 390.000 neue Schadprogramm- Varianten

Circa **11,1 Millionen Schadprogramme** für das Smartphone-System „**Android**“ (Stand: 2016)

Gezielte **Cyber-Spionage:**

Advanced Persistant Threats wird im Schnitt nach 243 Tagen entdeckt

Werkzeuge für **Cyber-Angriffe** gibt ab **5$ pro Stunde**

Manipulierte Werbebanner verbreiten **Drive-by-Exploits**. **2% aller Webseiten in Deutschland** sind damit verseucht.
Allein durch den Besuch einer solchen Website kann der Rechner infiziert werden

Täglich 2000-3000 Angriffe auf die Netze des Bundes, darunter **3-5 gezielte**

Ransomware:

Anstieg von Angriffsversuchen mittels Spam-E-Mail mit Verschlüsselungstrojaner im Anhang zwischen Januar und Mai 2016 um das **70 fache**

Gefährdungslage
Cyber-Sicherheits-Vorfälle: Auszug aus 2014-2016

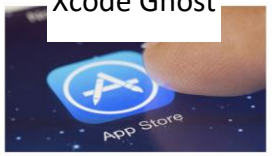

(6)


Adobe Systems
38 Mio. Kunden-datensätze

EBAY
145 Mio. Kunden-

(1)

Google
Stage Fright

Apple Store
Xcode Ghost


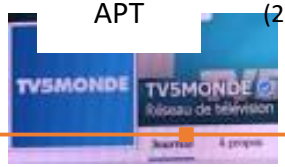
SWIFT
Bank (Bangladesh):
81 Mio$

(9)

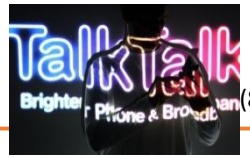

(4)

UKRAINE
Energy


(6)

TV MONDE
APT


(2)



(8)

RUAG (CH)
Cyber Spionage

TALK TALK
Kundenverlust: 100K
Schaden: £60 Mio

Heartbleed
OpenSSL


Shellshock
Bash

(3)
DD4BC
DDoS:
Finanz/Versicherungen


(6)

Feodo -> Geodo
Banking-Trojaner

Identitätsdiebstahl
16 Mio / 18 Mio

APT
Industrieanlagen


(4)

Dragonfly
Produktionsnetze

(5)

Deutscher Bundestag
APT

Ransomware
u.a. Krankenhäuser

CEO-Fraud

Bundesamt für Sicherheit in der Informationstechnik

2013 2014 2015 2016

(1) computerwoche.de
(2) faz.net
(3) bitcoinist.net
(4) Zeit.de
(5) power-technology.com
(6) web.de
(7) wikipedia.de
(8) theguardian.com
(9) Heise.de

Entwicklung der Gefährdungslage

Bedrohungen	2013	2014	2015	2016
Denial of Service (DoS, DDoS)	→	→	→	→
Botnetze	→	→	↗	↗
Spam	↘	↗	↗	→
Hacktivismus	→	→	→	→
Drive-by-Exploits (inc. Exploit- Kits)	↗	→	↗	↗
Schadprogramme	↗	↗	↗	→
Ransomware				↗
Identitätsdiebstahl	↗	↗	↗	→
Schwachstellen	↗	→	↗	→
Advanced Persistent Threats (APT)	↗	→	↗	↗

Gefährdungsbarometer ↗ steigend → gleichbleibend ↘ sinkend

Tabelle: Zusammenfassung der Gefährdungslage der Angriffsmethoden und -mittel

Angriff auf Funktionsfähigkeit der Bundeswehr

Cyberangriffe auf Deutschland

Experten sorgen sich um die Sicherheit der Datennetze von Bundeswehr und Bundesregierung. So wurde das IT-Netz der deutschen Streitkräfte im vergangenen Jahr 71 Millionen Mal von Hackern angegriffen. Das Datennetz der Bundesregierung wird rund 1,8 Millionen mal pro Jahr attackiert.

Frontal21 | 26.07.2016

Computerangriffe auf Streitkräfte Bundeswehr zählte 71 Millionen Cyberattacken 2015

Die Bundeswehr wurde im vergangenen Jahr offenbar millionenfach von Hackern attackiert. Mit einer eigenen Cyber-Truppe will das Verteidigungsministerium künftig zurückschlagen und sucht dafür IT-Experten.

Spiegel online | 16.03.2016

Im Visier von Hackern: 140 000 Cyber-Angriffe auf Bundeswehr …

2014 wurde das interne Netz der Bundeswehr knapp 6000 Mal ... Nach dem Cyber-Angriff auf TV5Monde wird überprüft, ob wieder die…

Bild.de | 14.04.2015

3. Das BSI – der IT-Sicherheitspartner

Leitsatz des BSI

Das BSI
als die nationale Cyber-Sicherheitsbehörde
gestaltet
Informationssicherheit in der Digitalisierung
durch Prävention, Detektion und Reaktion
für Wirtschaft, Staat und Gesellschaft.

IT-Sicherheitspartner für die Bundeswehr

Bundesamt
für Sicherheit in der
Informationstechnik

- Langjähriger *nationaler IT-Sicherheitsdienstleister/ – Gestalter und IT-Sicherheitsgarant* für Staat, Wirtschaft und Gesellschaft:
  Die Bundeswehr ist der größte Kunde des BSI im Bereich der technischen Prävention

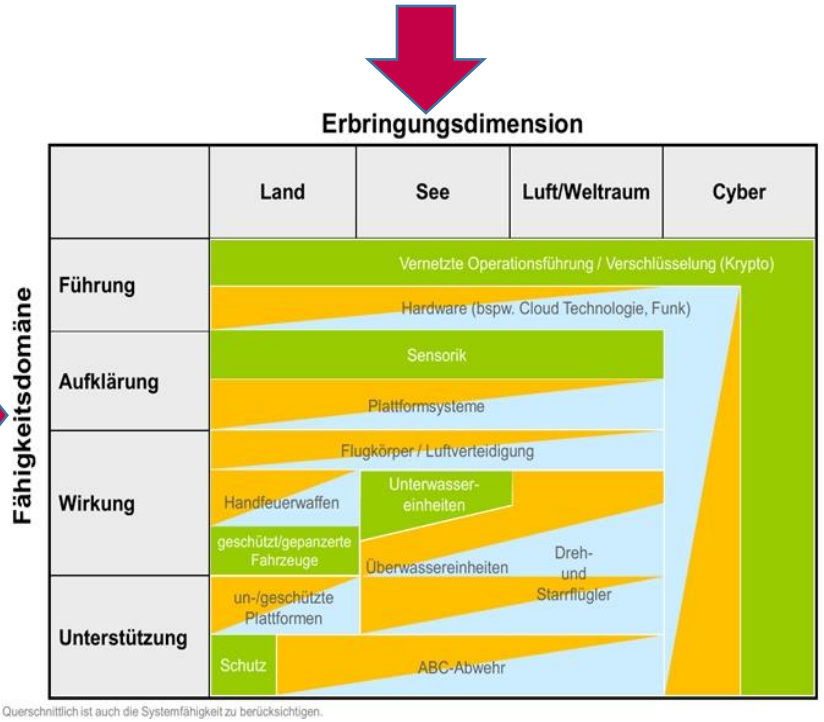
  Erfahrungsbasierte Gewährleistung des erforderlichen Innovationsvorsprungs für neue technologische IT-Sicherheitsherausforderungen bei
  - Kryptographie
  - Cyber-Sicherheit
- *IT-SiG - Umfangreiche Erweiterungen der Aufgaben und Zuständigkeiten des BSI in Zusammenarbeit mit der Bundeswehr*
  - CERTBund - CERTBw
  - Cyber-AZ

  sowie KRITIS-Vorfallsmeldestelle mit Vorfallsanalyse, Sicherheitsvorgaben, …

Kooperationsbereiche zwischen Bundeswehr und BSI

Prävention

- Steigerung von „Cyber-Resilienz“ durch IT-Grundschutz
- Ausrüstung der Bundeswehr mit hochwertiger Sicherheitstechnik zur Abwehr von Cyber-Hochwertangriffen
- IT-Sicherheitsberatung und Beratung zu IT-Sicherheitsarchitekturen
- Technologietrends für IKT in große vernetzte Organisationen
- Schutz der Wehrtechnischen Industrie als Angebot des BSI für Institutionen im besonderen staatlichen Interesse (INSI)-Bereich Rüstungsindustrie



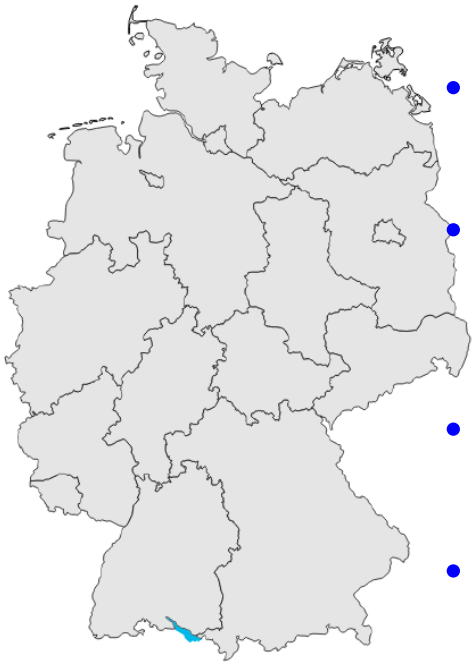
Quelle: Kabinettvorlage BMWi/BMVg Datenblatt-Nr. 18/09/100 S.7

Detektion und Reaktion

- bewährte Zusammenarbeit von CERTBund und CERTBw ausbauen
- Kooperation im Cyber-Az nach Aufstellung CIR intensivieren
- Einbeziehung der PEN-/Revisons-Teams der Bundeswehr in den Kreis der Reaktionskräfte zur technischen Bewältigung von Sicherheitsheitsvorfällen

4. Zusammenfassung und Ausblick

Ausblick - Gefährdungslage



- Nahezu *jede Behörde* und *jedes Unternehmen* ist Ziel von Cyber-Attacken, *ABER*: Nicht alle Angriffe werden entdeckt!
- *Dimension* der Cyber-Angriffe in Deutschland ist *besorgniserregend, die Ursachen* sind *vielschichtig*
- *Herausforderungen* an Detektion, Analyse und Bewertung sind extrem *hoch* und erfordern *herausragende Expertise*
- Viele Angriffe lassen sich durch *geeignete (Basis-) Präventionsmaßnahmen* verhindern
- Die Bundeswehr ist ein „*lohnendes Ziel*“ für Cyber-Angriffe
- *Eine abgestimmte Kooperation* zwischen *Bundeswehr* und *dem BSI* ist *erforderlich*

Bundesamt
für Sicherheit in der
Informationstechnik

Ausblick – Kooperation nach Neuaufstellung der Bundeswehr CIT/CIR

Etablierung der Plattform
„Forum Krypto- und Informationssicherheit“
in Zusammenarbeit von Bundeswehr und BSI

- Unterstützung & Kooperation zur Modernisierung der Kryptogeräte und Waffensysteme
- Personalaustausch zum Knowhow-Transfer und Beschleunigung der Prozesse
- Schließung von Fähigkeitslücken durch frühzeitige Einbindung des BSI bereits bei der Erstellung von Anforderungen
- Technologietrends für IKT in große vernetzte Organisationen

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Arne Schönbohm
Präsident

arne.schoenbohm@bsi.bund.de
Tel. +49 (0) 228 9582 - 5200
Fax +49 (0) 228 10 9582 - 5200

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de