Bundesamt
für Sicherheit in der
Informationstechnik

Lageerkenntnis – Voraussetzung einer erfolgreichen Gegenstrategie

Klaus Keus, Dipl. Math.
Referatsleiter:
Cybersicherheit und Kritische Infrastrukturen: IT-Sicherheitslagebild

Bundesamt für Sicherheit in der Informationstechnik

18. Nov. 2016, Fachgruppe SECMGT, Frankfurt

Motivation

„Wer die *aktuelle Cyber-Sicherheits-Lage nicht* ausreichend *kennt*, weiß vielfach nicht, wie er sich *effektiv* und *nachhaltig* gegen potenzielle Cyber-Sicherheits-Angriffe *schützen* kann.“

*) unnamed IT-Security Expert

1. Ausgangssituation: Informationstechnik heute und zugehörige Gefährdungslage

Informationstechnik heute:
vernetzt, komplex, allgegenwärtig

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

Technologische Durchdringung und Vernetzung: Alle physische Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden , z.B.: IoT, Automotive, ...)

Komplexität: Die Komplexität der IT nimmt durch vertikale und horizontale Integration in die Wertschöpfungsprozesse erheblich zu, z.B.: Industrie 4.0, Infotainment, Gesundheit (eHealth), ...)

Allgegenwärtigkeit: Jedes System und jede Information ist praktisch zu jeder Zeit und von jedem Ort über das Internet für unterschiedlichste Plattformen für jedermann erreichbar , z.B.: Smart City, Smart Home, ...)

Gefährdungslage:

Wandel der Bedrohungslage - Herausforderung für alle

Lagebild Cyber-Sicherheit

Cyber-Angriffe heute:

- *komplexer* und *mehrdimensionaler*
- *vielfältiger* (ungezielte Breitenangriffe / gezielte Angriffe / APT-Angriffe (Behörden, Rüstungsunternehmen))

Angreifer

- *professioneller*
- *verbessern* ihre (monetäre) *Erfolgsaussichten*

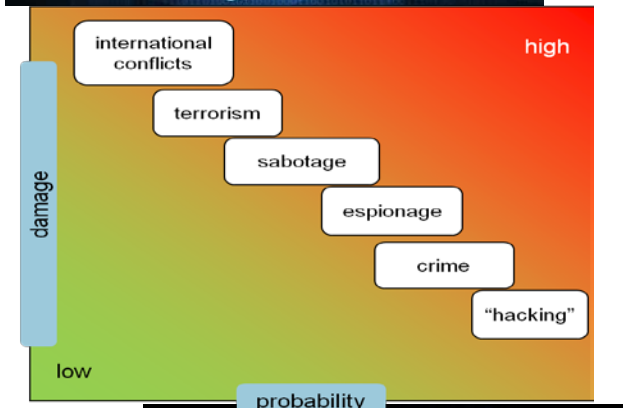
Änderung von Rahmenbedingungen führen zu *verstärkter Asymmetrie zwischen Angriff und Verteidigung* zum Vorteil der Angreifer:

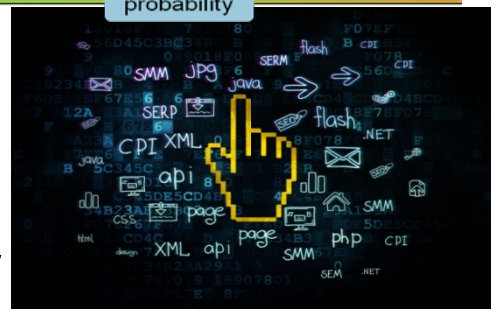
- neue technologische Angriffsmöglichkeiten
- zunehmende Komplexität der Technologie
- Unbedarftheit der Nutzer
- Überforderung der Nutzer

2. Ursachen und Wirkungen der aktuellen Cyber-Gefährdungs- und Bedrohungslage

Gefährdungslage:

Wandel der Bedrohungslage - Herausforderung für alle





Cyber-Angriffe sind *komplexer* und *mehrdimensionaler* (Kombination und Vielfältigkeit der unterschiedlichen Angriffsvektoren) geworden.

Angreifer werden professioneller, zunehmend professioneller, international vernetzt mit Aufgabenteilung, verbesserte Reaktion der Täter/Angreifer auf verbesserte Abwehr (Ping-Pong-Effekt), Ausdehnung der Motivationsbandbreite der Angreifer

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

Gefährdungslage:

Wandel der Bedrohungslage - Herausforderung für alle

Cyber-Angriffe – (beinahe) ein Alltagsphänomen? !

Cyber-Angriffe auf

- Unternehmen
- Verwaltungen
- Privatnutzer

kommen jeden Tag vor.

Cyber-Angriffe haben die Phase einer *ernsthaften Bedrohung und Gefährdung* unserer Wirtschaft, Verwaltung und Gesellschaft erreicht.

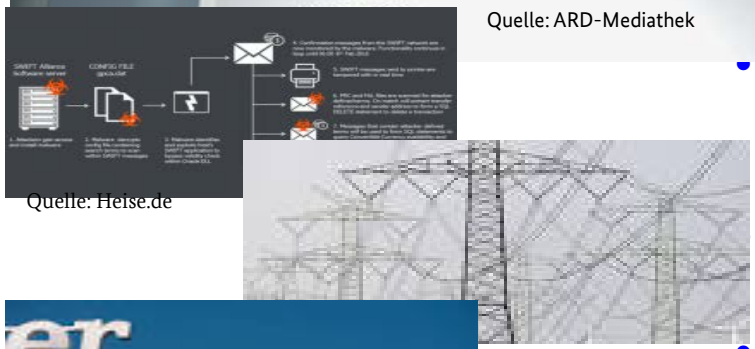
Dies gilt auch für *Deutschland.*

Cyber-Angriffe sind heute keine unvorhersehbaren Überraschungen mehr!

Beispiele zur aktuellen Wirkung –

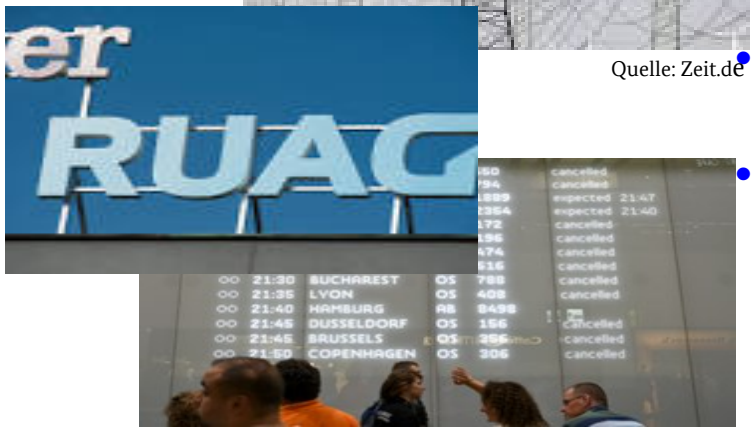
Angriffe 2016: Auszug

Quelle: ARD-Mediathek



Quelle: Heise.de

Quelle: Zeit.de



Quelle: apa

Health:

- 02/16: Ransomware–Virus legt Krankenhaus lahm

Finanz:

- 05/16: Cyber-Angriff auf Zentralbank Bangladesch - 81 Millionen Dollar erbeutet (SWIFT)

Energie:

- 12/15: Angriff auf Stromversorgung Ukraine
- 04/16: Atomkraftwerk Gundremmingen

Rüstung:

- 1. HJ 16: Cyberspionageangriff auf Rüstungsunternehmen RUAG (CH)

Transport:

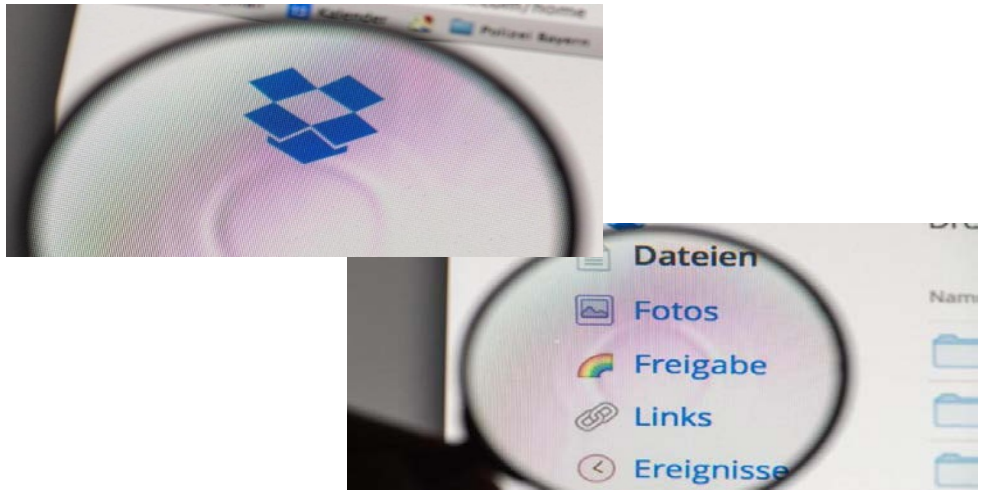
- 09/16: DDoS Angriff auf den Flughafen Schwechat

... DDoS-Erpressungen, Ausspähen E-Mailzugangsdaten Politiker, ...

‚Alte‘ Ursache und aktuelle Wirkung –

Nachhaltigkeit an Beispielen von Identitätsdiebstahl

Lagebild Cyber-Sicherheit



Dropbox:

- 68 Mio. verschlüsselte, echte Passwörter
- Hack: 2012
- Veröffentlichung: 09/2016

Yahoo: Weltrekord ?

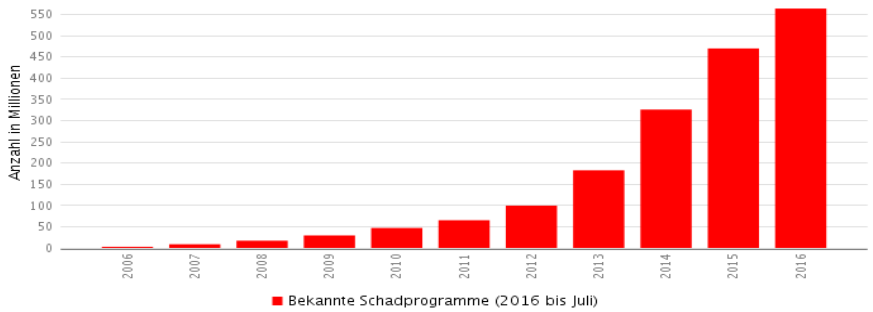
- Mindestens 500 Mio. Benutzerkontendaten gestohlen
- 200 Mio. Login-Daten von Yahoo-Nutzern im Netz
- Hack: Ende 2014
- Veröffentlichung: 09/2016

3. Aktuelle Gefährdungslage - Überblick und Ausschnitt

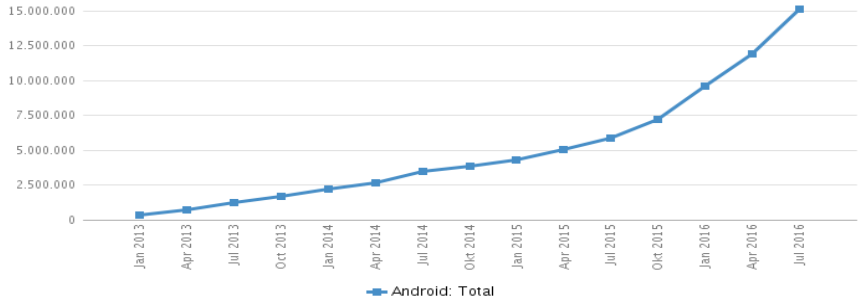
Schadprogramme

- **Bedrohungs-Lage** ist weiterhin **hoch,** steigt stetig an
- Aktuell: **Bedrohung** durch **Ransomware** sehr hoch
- neue Varianten in immer kürzeren Abständen **erschwert die Erkennung** durch AV-Produkte
- **Täglich** werden **mind. 390.000 neue** Schadprogramm-Varianten, **Gesamt** mehr als **560 Mio**
- **Zeitspanne** zur Erkennung neuer Malware: mehrere **Stunden bis zu Tagen**
- **Windows-Plattformen:** am häufigsten betroffen.
- **Android**: ca. **15 Mio** verschiedene Schadprogramme, Trend steigend (Verdoppelung in 1 Jahr)
- **mobile Endgeräte**: fast ausschließlich für Android-Plattformen
- fast ausschließlich in **alternativen App Stores** mit stark zunehmender Tendenz, teilweise auch in **offiziellen App Stores**

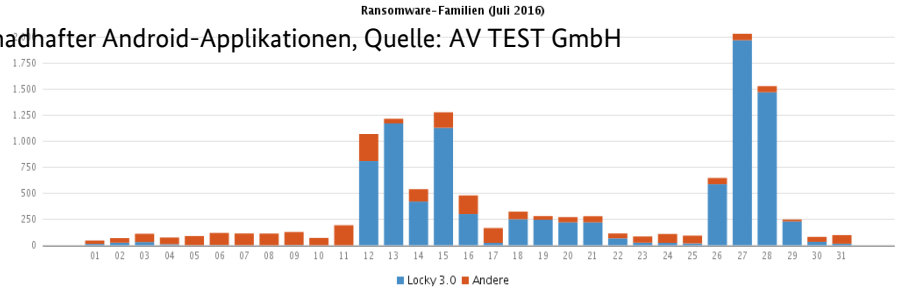
Lagebild Cyber-Sicherheit



Bekannte Schadprogramm-Varianten



Anzahl schadhafter Android-Applikationen, Quelle: AV TEST GmbH



Ransomware-Familien, Quelle: BSI, Stand: Juli 2016

Ransomware

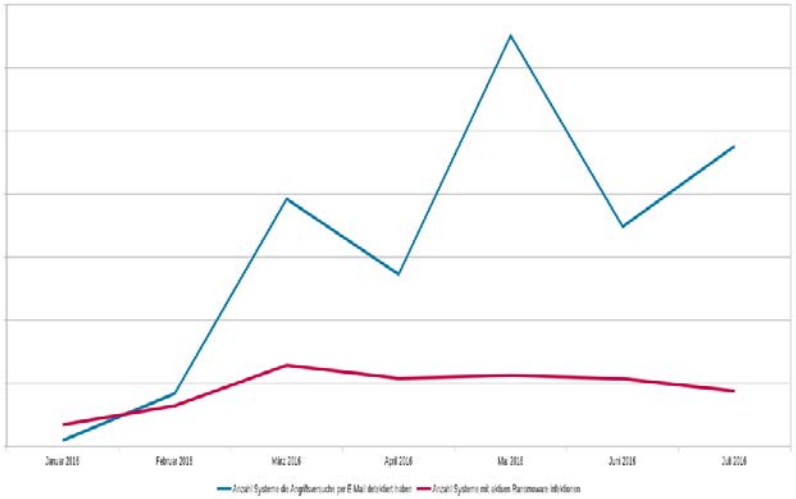
Lagebild Cyber-Sicherheit

Vorteile für Angreifer gegenüber anderen Angriffen:

- ***Geringes Entdeckungsrisiko*** wg. anonymer Bezahlung per Bitcoin
- ***Höherer Gewinn***, da keine Mittelsmänner oder Warenagenten notwendig (deshalb z. B. Umwandlung von ‚Dridex' vom Banking- zum Ransomware-Schadprogramm)

Ransomware:

- Umfrage der Allianz für Cyber-Sicherheit 2016: ***32%*** der antwortenden Unternehmen ***von Ransomware betroffen***
- Meist ***Massenangriffe***, selten gezielte Angriffe
- ***Fast 2/3*** der per Spam verteilten Ransomware entfallen auf ‚***Locky***'



Trend der Anzahl Systeme mit Ransomware-Detektionen von Virenschutzprogrammen in D seit 01/16

APT

Lagebild Cyber-Sicherheit

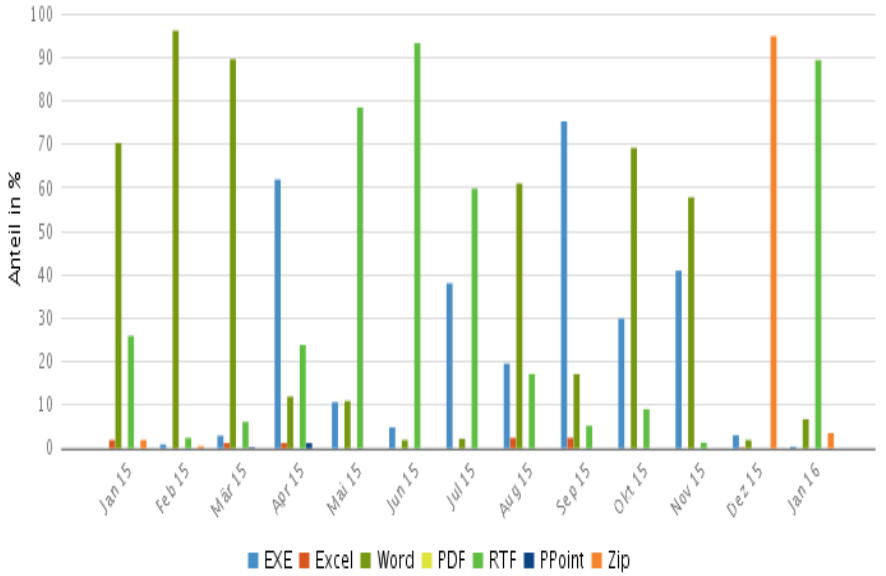
Advanced Persistent Threats

- Auf westliche Unternehmen: ***starke Abnahme*** in ***2015, 2016*** auf ***niedrigem Niveau*** verbleibend

- ***Fokus derzeit***: Südostasien, Russland, Ukraine + Regionen mit zwischenstaatlichen Konflikten

- ***Ziele***: Regierungseinrichtungen, Rüstungsunternehmen, regierungskritische Personen

- Aufgrund des höheren Kenntnisstandes und der im Regelfall sehr professionellen Vorgehensweise des Angreifers stellen ***APTs eine ernstzunehmende Bedrohung für die IT-Sicherheit einer Behörde oder Firma*** dar. Kenntnis über einen erfolgten Angriff erhält der Angegriffene häufig erst durch externe Quellen und immer nach relativ langer Zeit



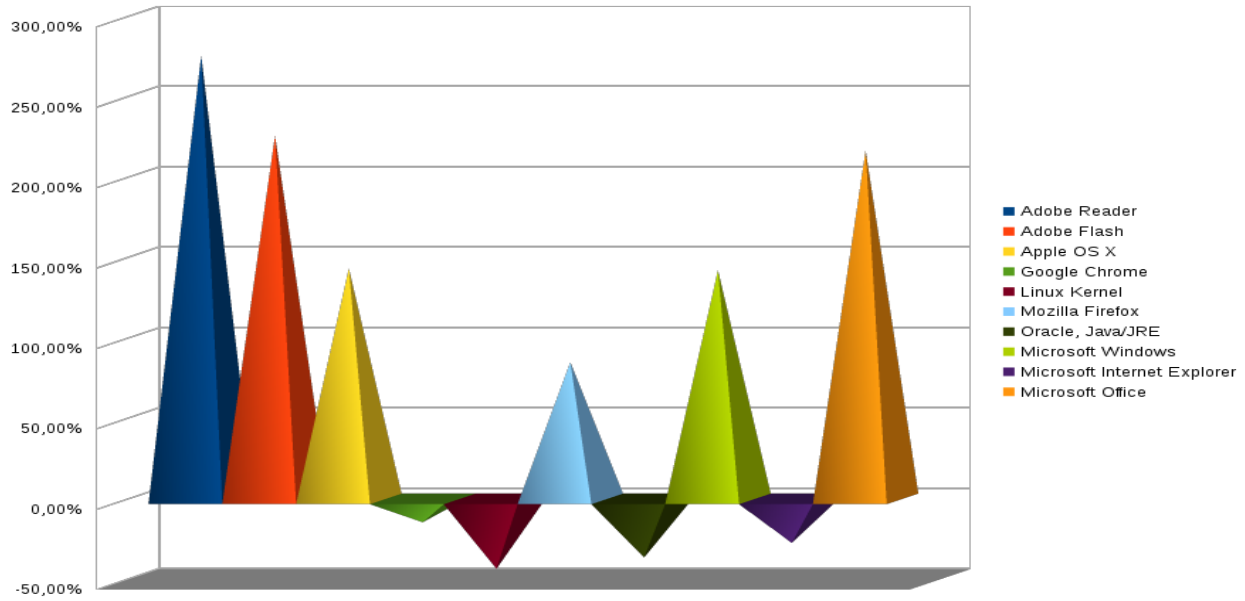
SW-Schwachstellen

Lagebild Cyber-Sicherheit

Software-Schwachstellen

- **Entwicklung der Anzahl** der **geschlossenen Schwachstellen** in den betrachteten Produkten **stark unterschiedlich**

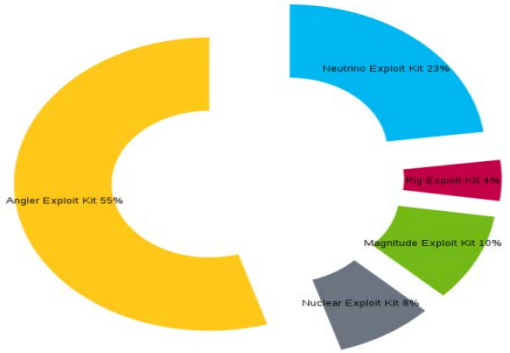
- **Höhere Gefährdung** nur bei **Adobe Flash** beobachtet, da Schwachstellen breit ausgenutzt werden



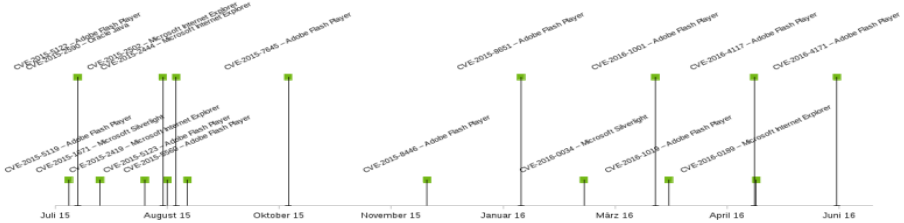
Drive-By-Exploits

Lagebild Cyber-Sicherheit

- **anhaltend hohe Gefährdung** durch Drive-by-Exploits und Exploit-Kits
- weiterhin **regelmäßig unbekannte** oder **neue** Schwachstellen für Drive-by-Angriffe verwendet oder in Exploit-Kits integriert
- In **gezielten** als auch **ungezielten Angriffe**, beispielsweise durch Malvertising,
- **Angriffsversuche** finden **regelmäßig** statt, auch in Deutschland.
- **Summe der Detektionen** von Exploit-Angriffen in Deutschland ist auf **gleichbleibendem Niveau** (06/16: im Durchschnitt täglich ca. 1120 Angriffsversuche)



Verteilung der Exploit-Kit-Detektionen nach Exploit-Kit
Zeitraum 03 – 06/16 in D

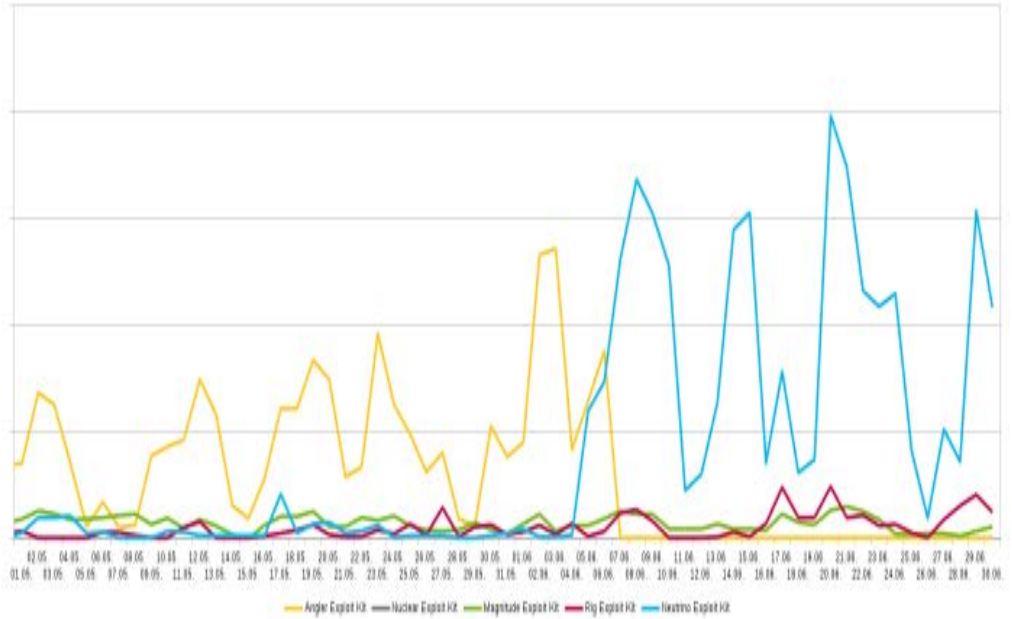


Verwendung neuer Schwachstellen in Drive-by-Angriffen
und Exploit-Kits der letzten 12 Monate

Drive-By-Exploits

Lagebild Cyber-Sicherheit

- Angriffe durch Drive-by-Exploits die **zweithäufigste Ursache für Ransomware-Infektionen** in deutschen Unternehmen
- **Aktuelle Angriffskampagnen** mit Exploit-Kits infizieren Nutzer in Deutschland u.a. mit Ransomware (Datenverluste, finanzielle Schäden)
- **Exploit-Kit-Markt sehr flexibel**: etablierte werden umgehend durch andere ersetzt
- aktuelle Lage erfordert das **sofortige Einspielen von Sicherheitsupdates** nach deren Bereitstellung
- Vollständige und schnelle **Patch-Management-Prozesse** sind unerlässlich



Verlauf der Exploit-Kit-Detektionen von März bis April 2016 in Deutschland

Identitätsdiebstahl

Lagebild Cyber-Sicherheit

- Dem BSI sind durchgehend ca. **50.400 Infektionen durch Schadprogramm-Familien mit Identitätsdiebstahlfunktionen** in D bekannt (akt. Stand 10.16)

- **Gesamtzahl** der Infektionen liegt **erheblich höher**:
  - da die verwendete Messmethode nur einen Bruchteil der Infektionen erfasst
  - Es existieren über die hier erfassten Schadprogramm-Familien hinaus weit mehr Schadprogramme mit Identitätsdiebstahlfunktion
  - 09/2015 – 08/2016: Analyse von ca 123.000 neuen Schadprogramme mit Bezug zu Identitätsdiebstahl in D

Infektionen mit Schadprogrammen mit Identitätsdiebstahlfunktion in Deutschland (gleitender 6-Monats-Durchschnitt), Quelle: BSI, Stand: August 2016

DDoS

- **Anzahl:** mehr als **160 Angriffe pro Tag**

- **Angriffsbandbreite:** maximal beobachtet: 803,57 Gbps (**gestiegen um 70%**), Durchschnitt in D: 1,0 Gbps bis ca. 1,5 Gbps, > 800 Gbps in Einzelfällen (z.B. Mirai, Brian Krebs Block etc.)

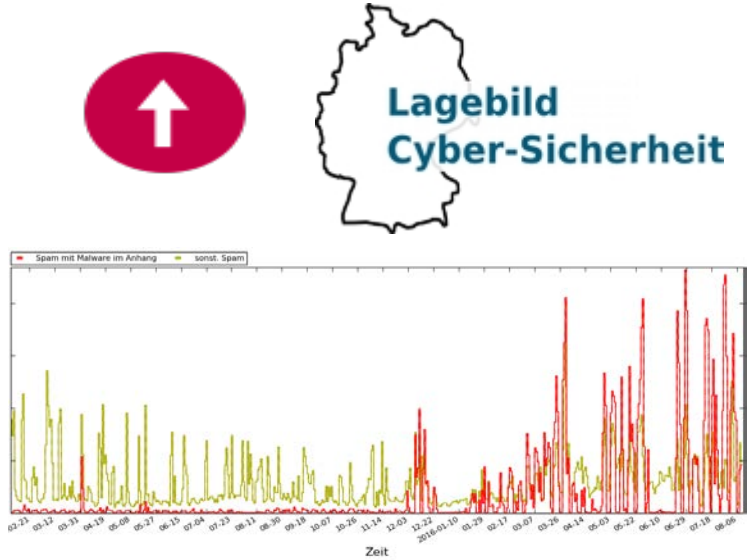
- **Angriffsmethoden:** Botnetz-Angriffe, Reflection Angriffe (DNS, NTP (rückläufig), CHARGEN, UDP-basiert)

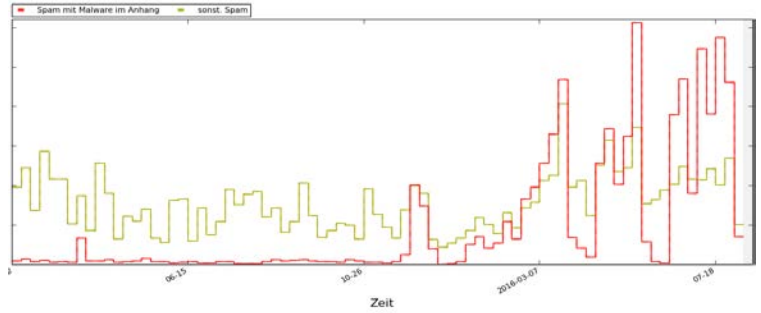
- **Motivation:**
  - **Sabotage** (politischen bzw. ideologischen Auseinandersetzung),
  - **Manipulation** bzw. **Störung** von Online-Games bzw. Online-Wetten,
  - **Vandalismus** bzw. Demonstration von DDoS Fähigkeiten

- **Dauer / Durchschnittliche Dauer:** Wenige Minuten – mehrere Tag, Durchschnitt 30 – 40 Minuten

SPAM

- **Quellen**: Entwicklungs- und Schwellenländern (Indien, Vietnam, Mexiko, u. a.).
- **Form**: Dropper vs. Downloader (Vielfach: Neuentwicklungen / Weiterentwicklungen)
- **hohe Wirksamkeit der Verteilung** von Schadprogrammen über Spam (dazu siehe auch Ransomware und Malware)
- **bis dahin weitgehend verborgen**, da die bis dato verteilte Schadsoftware recht unauffällig, keine Detektion durch Nutzer
- Anstieg von Malware-Spam: **profitables Cyber-Crime Geschäft**
- Schadsoftware-Spam ist weiterhin eine der **Hauptquellen von Malware-Infektionen**





Cyber-Sicherheitslage:
Gesamtüberblick (Oktober 2016)

Ursachen → **Wirkungen**

- Täglich 390.000 neue Schadprogramm-Varianten
- Ca. 15 Mio. Schadprogramme Android
- Gesamt: Über 560 Mio. Schadpro-gramme
- Ransomware: Anstieg um Faktor 70 seit 01/16
- Allzeithoch Spam-Malware: (12.2015) 30% des gesamten Mailverkehr
- DDoS-Angriffe: Buy/rent a Bot: 30-70 $/Tag
- Identitäts-diebstahl: 56.000 in D bekannte Infektionen
- Hacktivismus: Stark zunehmend

- Defacement: 980 Web-Seiten in D, 108.000 weltweit
- Yahoo: Datengau mit rund 500 Mio. betroffene Kunden erforderlich
- DDoS: Ca. 1,0 Gbps bis 1,5 Gbps pro Angriff
- APT: vor allem in Konfliktregionen
- APT28: Angriff auf MdB mittels gefälschter Webmail-Server
- DDoS: auf KRITIS-Untern. + Behörden
- IVBB: 3600/Tag gesperrte Verbindungen zu Schadcode-servern
- 1 gezielter Angriff / Wo auf **BV** mit nachrichtl. Hintergrund
- Verdoppelung Schadprogramme für Android in einem Jahr
- Zunahme ungezielter Ransomware-kampagnen
- Angreifer-Fokusier-ung auf Ransom-ware statt Identitätsdiebstahl

4. Prognose der Weiterentwicklung - anhand von 2 Beispielen

Ransomware–Prognose:

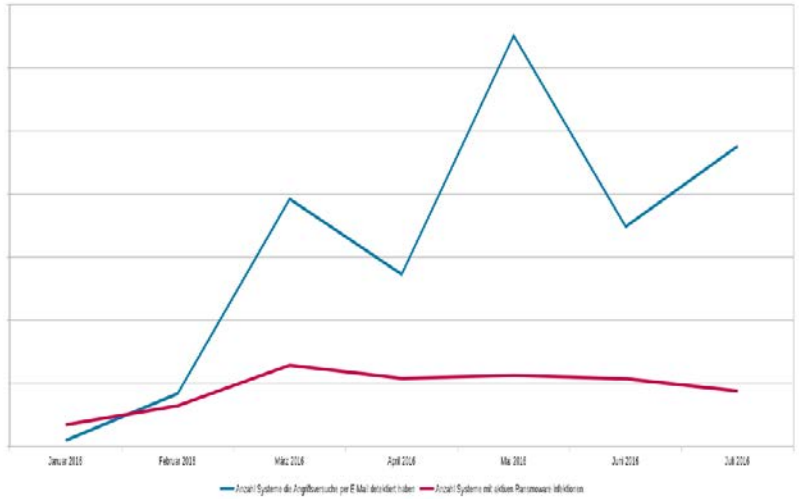
Lage, Daten, Fakten

Lagebild Cyber-Sicherheit

Bedrohung des Jahres: Ransomware

- **Anstieg** der Bedrohung durch Spam-Kampagnen seit Januar 2016: **Faktor 70** (blau)

- **Anzahl** Infektionen **konstant** (rot)



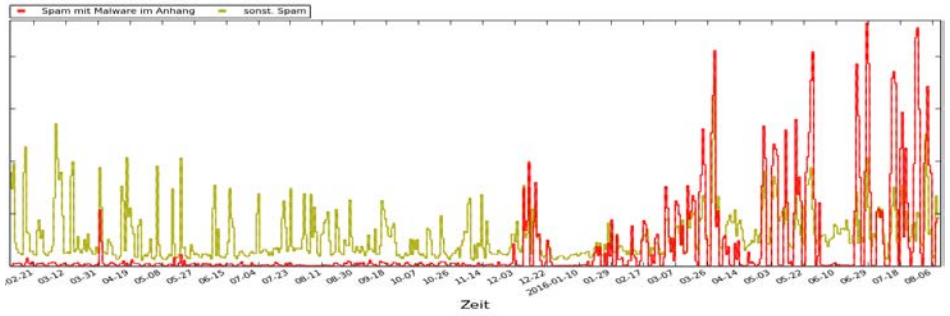
Trend der Anzahl Systeme mit Ransomware-Detektionen von Virenschutzprogrammen in D seit 01/16

SPAM-Prognose

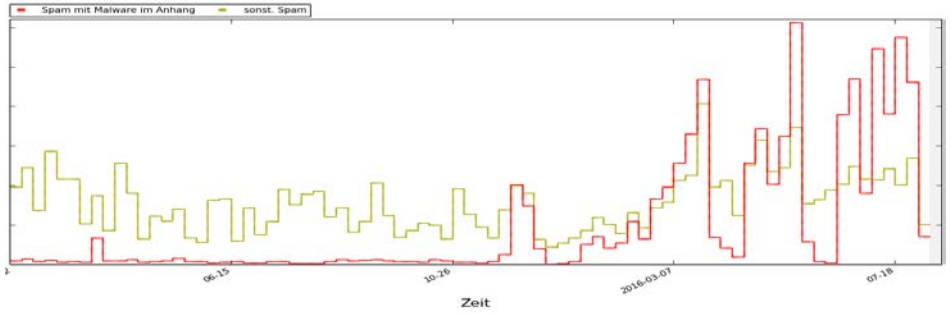
Lage, Daten, Fakten

Lagebild Cyber-Sicherheit

- **Volumen** von **Spamnachrichten mit Schadsoftware** im Anhang seit 12/15 sprunghaft **angestiegen** (Zunahme 1. HJ 16: ca. +73 %), zum Vergleich: klassischen Spams: ca +16%,



- **Anzahl: 1.270 % Zunahme** der Spam-Nachrichten mit Schadsoftware im Anhang



Prognose auf Basis Befragung:
Umkehrtrend nicht erkennbar

Lagebild Cyber-Sicherheit

Allianz für Cyber-Sicherheit

	2014/2015 (%)	2016 (%)
War die Institution der Befragten in den Jahren 2014 und 2015 das Ziel von Cyber-Angriffen?	58.5	65(+6)
Waren die in den Jahren 2014/2015 festgestellten Cyber-Angriffe erfolgreich?	42,7% erfolgreich 42,3% erfolgreich abgewehrt 11,3% mit Schaden mehr als jede 4. Institution betroffen (31,5%)	47 (+4) 44 (+1) 7 (-4) Jede 3. Institution
Innerh. der letzten 6 Mo. Ransomware-Infektion	32 (Umfrage 04/16)	32

Prognose Cyber-Sicherheitslage:
Auszug aus ACS-Umfrage 2014 – 2015 – 2016 (09.16)

War Ihre Institution schon einmal das Ziel eines erfolgreichen Cyber-Angriffs?

2016	2015
12% relevant / 39%	10%

Schäden?

2016
5%: schwerwiegend/ erheblich: **17% Reputation, 32% Produktionsausfall / Betriebsausfall** **7% Diebstahl sensitiver / wirtschaftl. bedeutender Daten**

Prognose Cyber-Sicherheitslage:
Auszug aus ACS-Umfrage 2014 – 2015 – 2016 (09.16)

Stellen Cyber-Angriffe eine relevante Gefährdung für die Betriebsfähigkeit Ihrer Institution dar?

2016	2015
47% JA	46% JA

Änderung der Bewertung der Risiken durch Cyber-Angriffe?

2016	2015
77% JA	70% JA

Sind die in Ihrer Institution getroffenen Maßnahmen zum Schutz gegen Cyber-Angriffe ausreichend?

NEIN	Ja
80%	16%

➔Cyber-Angriffe sind keine unvorhersehbaren Überraschungen!

5. BSI als Partner zielgerichteter Gegenmaßnahmen: Lagebildprodukte und andere Instrumente

5.1 Lagebild IT-/ Cybersicherheit

IT-/ Cyber-Sicherheitslagebild

ein multilateraler Ansatz mit unterschiedlichen Zielgruppen:

- Anwender
- Provider und Diensteanbieter
- IT-Branche und Hersteller
- Politik
- BSI

IT-/ Cyber-Sicherheitslagebild
Technische Lageinformationen

- Das BSI verfügt über eine **Vielzahl von technischen Informationen** über die Cyber-Sicherheitslage
  - **Lagezentrum**
    - Vorfallsmeldungen und -bearbeitung
    - Auswertung öffentlicher Nachrichtenquellen
  - **Statistiken und Detektionsdaten**
    - Regierungsnetze
    - Vertragspartner
    - Partner der Allianz für Cyber-Sicherheit

IT-/ Cyber-Sicherheitslagebild

Ziel / Zielerreichung

Lagebild Cyber-Sicherheit

Ziel:

- ❒ Nachhaltige Verbesserung der Cyber-Sicherheit in D
- ❒ Argumentationshilfen für die Bereitstellung von Ressourcen durch Risikodarstellung (Sensibilisierung)
- ❒ Aufzeigen von lagespezifischen Maßnahmen für Management, CISO, Administratoren
- ❒ Auslösen akuten Handlungsbedarfs
- ❒ Frühwarnung noch nicht betroffener Bereiche
- ❒ Ableiten des präventiven/reaktiven Handlungsbedarfs
- ❒ Ableiten eines politischen Handlungsbedarfs

Zielerreichung durch:

- ❒ Laufend aktualisierte Themenlagebilder
- ❒ Analyse der Ursachen
- ❒ Risikodarstellung
- ❒ Handlungsempfehlungen

3 Aktuelle Verteilung von Exploit-Kits in Deutschland

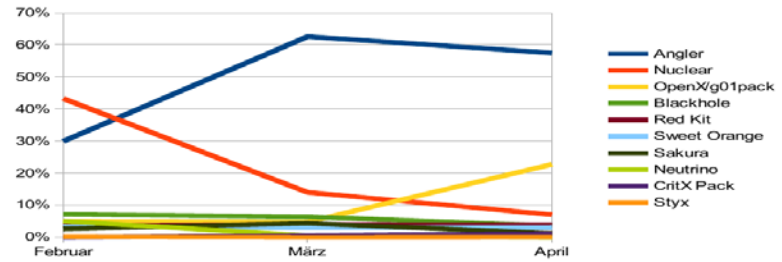


Abbildung 3: Top 10 Detektionen von Exploit-Kits in Deutschland in den Monaten Februar 2014 – April 2014 (Quelle BSI)

IT-/ Cyber-Sicherheitslagebild

Adressaten

Institutionen, die **potenzielles Angriffsziel** darstellen können:

- ❒ Verwaltung (Bund, Land, Kommunen)
- ❒ Wirtschaft (KRITIS, INSI, KMU)

Institutionen, die **mittelbaren Einfluss** besitzen auf IT-Sicherheit:

- ❒ Aufsichtsbehörden
- ❒ Forschungseinrichtungen
- ❒ Provider
- ❒ Dienstleister für Cyber-Sicherheit
- ❒ Hersteller von Cyber-Sicherheitsprodukten
- ❒ Politik
- ❒ Medien

IT-/ Cyber-Sicherheitslagebild

Zielgruppen - Hierarchieebenen -

Lagebild Cyber-Sicherheit

IT-/ Cyber-Sicherheitslagebild

Quellen

Lagebild Cyber-Sicherheit

Quellen des Bundes

- ✓Lagezentrum
- ✓Netze des Bundes
- ✓Meldestelle

Quellen der Allianz

- ✓Partner der Allianz
- ✓gemeldete Vorfälle

Allianz für Cyber-Sicherheit

Sonstige Quellen

- ✓CERTs
- ✓Hersteller
- ✓Dienstleister
- ✓andere kostenlose (OpenSource) oder
- ✓Kostenpflichtige Quellen (z.B. Forschung)

Lagebild Cyber-Sicherheit

IT-/ Cyber-Sicherheitslagebild

Themenlagebilder

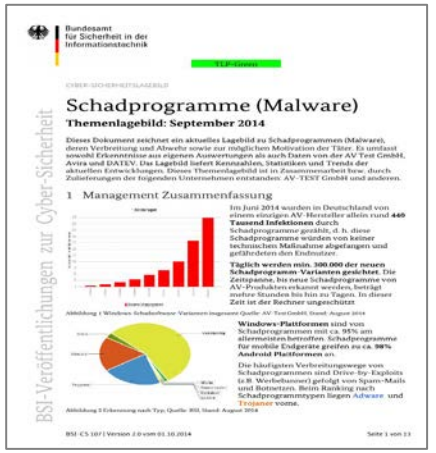
Lagebild Cyber-Sicherheit

Technische Ursachen für Cyber-Angriffe
- ❒Themenlagebild: **Schwachstellen**

Cyber-Angriffsmittel
- ❒Themenlagebild: **Schadprogramme (Malware)**
- ❒Themenlagebild: **Botnetze**
- ❒Themenlagebild: **Drive-by-Exploits**
- ❒Themenlagebild: **Exploit-Kits**
- ❒Themenlagebild: **Diebstahl und Missbrauch von Identitäten**

Auswertung der Vorfälle im Bereich Flächenangriffe und gezielte Angriffe
- ❒Themenlagebild: **Spam**
- ❒Themenlagebild: **DDoS**
- ❒Themenlagebild: **Gezielte Angriffe (APT)**

Täterorientierte Cyber-Sicherheitslage, Hacktivismus und Malware-Autoren
- ❒Themenlagebild: **Hacktivismus**


Bundesamt für Sicherheit in der Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

Schadprogramme (Malware)

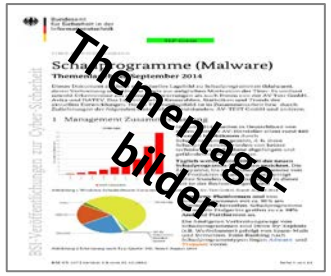
Themenlagebild: September 2014

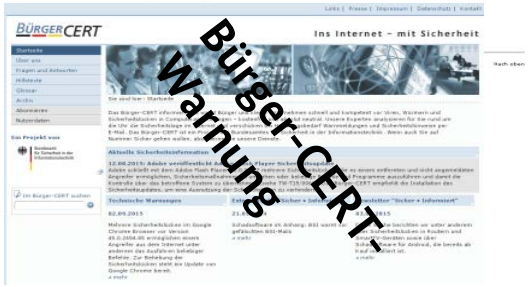
1 Management Zusammenfassung

Federal Office for Information Security

Information-Sharing:
Lageberichte / Lagebilder: Auszug aus Produktübersicht

Lagebild Cyber-Sicherheit





ABER: Alle Lagebilder teilen immer ein Problem

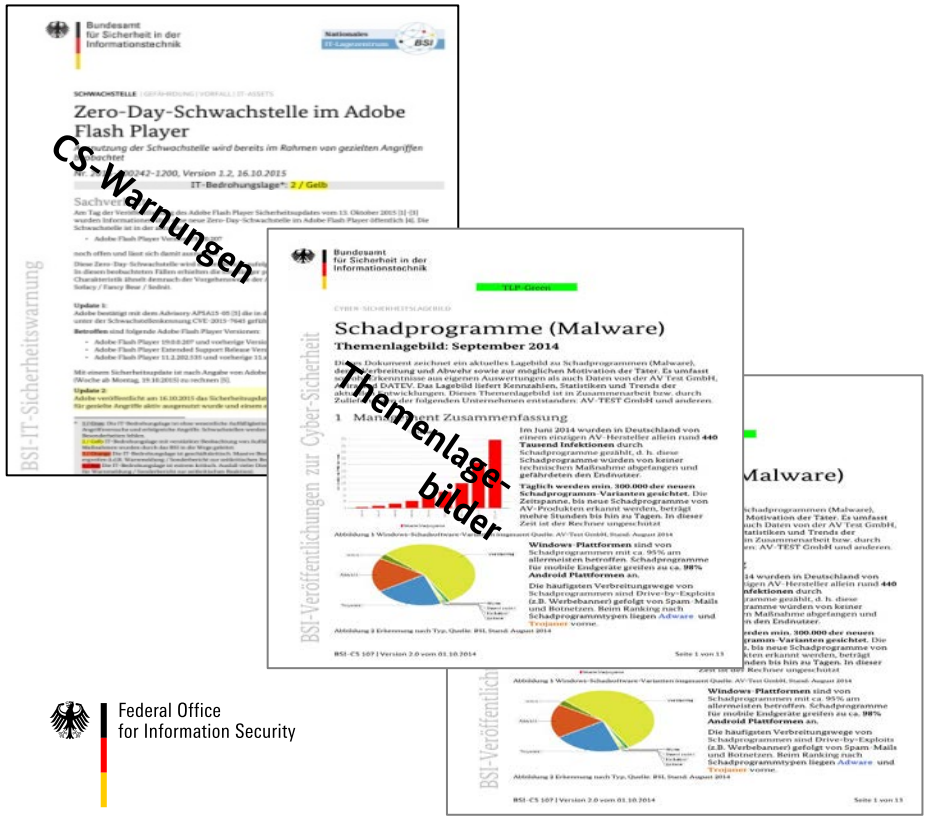
Bild: © niyazz – Fotolia.com

5.2 Weitere Instrumente

Allianz für Cyber-Sicherheit –
Instrument I - PPP Modell ACS

Lagebild Cyber-Sicherheit

Allianz für Cyber-Sicherheit



Intensivierte Einbindung kompetenter **Vertreter der Wirtschaft** als *aktive Partner* der BSI-Wirtschafts-Partnerschaft *Alliance für Cyber-Sicherheit* (ACS), ***z.B. VW AG*** *als initiierendes Mitglied eines zukünftigen ACS-AK , Cyber Security in der Automobilindustrie' unter Beteiligung des VDA und anderer Vertreter der Automobilindustrie!*

Einbindung in den *Informationsaustausch* des BSI mit der Wirtschaft zur *IT-Sicherheitslage* und *Zugriff* der **Unternehmen** auf die unterschiedlichen *Lagebild-Produkte* des BSI

Federal Office for Information Security

Das BSI als Kooperationspartner -

Instrument II - ausgewählte bilaterale Absichtserklärungen (Beispiel 1)

Lagebild Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik

VOLKSWAGEN

Absichtserklärung

Verbesserung des Lagebildes zu Cyber-Sicherheit

zwischen
dem

Bundesamt für Sicherheit in der Informationstechnik (BSI)

und der

Konzernsicherheit Volkswagen AG

Untermauerung und Ausdruck der *Kooperationsabsichten* durch bilaterale *Absichtserklärungen,* z.B. *zur Verbesserung des IT-Sicherheits-Lagebilds*

Beispiel: zwischen Konzernsicherheit Volkswagen AG und *BSI*

Das BSI als Kooperationspartner –

Instrument II - ausgewählte bilaterale Absichtserklärungen (Beispiel 2)

Flankierende Kooperationsmaßnahmen des BSI mit *DCSO*, z.B. im Kontext der

- Cyber Threat Intelligence (Lagebild-Informationen)
- Produktevaluierung / -Bewertung

UP-Kritis – Vision

Lagebild Cyber-Sicherheit

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

6. Zusammenfassung: Lage und Ausblick

Gefährdungslage
Zusammenfassung

- *D* ist ein *bevorzugtes Ziel* für Cyber-Angriffe und e-Spionage, dies betrifft auch die Produktionswirtschaft
- nahezu *jeder Wirtschaftszweig* und *jedes Unternehmen* ist Ziel von Cyber-Attacken, *ABER*: Nicht alle Angriffe werden entdeckt!
- *Dimension* der Cyber-Angriffe in Deutschland ist *besorgniserregend*
- *Ursachen* sind *vielschichtig*
- Cybersicherheitsangriffe sind *keine unvorhersehbaren Überraschungen* mehr.

Gefährdungslage

Lösungsansatz / Ausblick

Unternehmen und Behörden müssen handeln ! Viele Angriffe lassen sich durch *geeignete (Basis-) Präventionsmaßnahmen* verhindern

IT-Sicherheit muss *Teil* eines ganzheitlichen *Risikomanagements* sein

Abgestimmte Kooperation einschließlich *Informationsaustausch* zwischen *Behörden, Wirtschaft* und *zuständigen Behörden (BSI)* ist zwingend *erforderlich*

Das BSI bietet verschiedene Instrumente und Maßnahmen in einer *ganzheitlichen Strategie koordinierter Gegenmaßnahmen*

IT-SiG und seine Wirkung sind ist ein Schritt in die richtige Richtung

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:

Klaus Keus, Dipl. Math.
Referatsleiter
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Tel.: +49 (0)228 99 - 9582 - 5141
Fax: +49 (0)228 99 - 10 - 9582 - 5141
Klaus.Keus@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de