Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild
Cyber-Sicherheit

Die Lage der IT-Sicherheit in Deutschland –

Am Spiegel des nationalen Lagebilds Cybersicherheit

Dipl. Math. Klaus Keus
Referatsleiter „Cyber-Sicherheit: Analyse und Prognose“

Bundesamt für Sicherheit in der Informationstechnik

ZKI Frühjahrstagung:
„Entwicklung einer hochschulweiten IT-Architektur mit Open Source“

09.-11.03.2015,
Heinrich-Heine-Universität Düsseldorf

Agenda

- Hintergründe: **Ursachen** und **Parameter** der aktuellen Gefährdungs- und Cyber-Sicherheitslage
- Lösungsansatz: 'Aus der Praxis für die Praxis': **Lagebild Cyber-Sicherheit**
- **OpenSource vs Proprietär-SW** im Spiegel des Lagebilds
- **Fazit** und **Zusammenfassung**

Cyber-Sicherheitslage:
Ursachen

- **Technische Komplexität, Vernetzung** und **Vielfalt**
- **Komplexität** und **Sicherheitsbewusstsein**
- **Informationsaustausch** und zugeh. **Nutzung**
- Geringes **Entdeckungsrisiko**

Cyber-Sicherheitslage:
Parameter

Cyber-Sicherheitslage ist bestimmt durch

- **Ursachen** (Technologie, Verhalten)
- **Angriffsmittel** und **-Methoden** (Vielfalt der Technologischen Mittel und Methoden)
- **Angreifer / Täter**
- **Wirkungen**

Cyber-Sicherheitslage:
Lösungsansätze

ein **multilateraler Ansatz** mit unterschiedlichen Zielgruppen:

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

Bundesamt
für Sicherheit in der
Informationstechnik

Konkreter Lösungsbeitrag des BSI

Lagebild
Cyber-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit:
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

Zielerreichung durch:

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

3 Aktuelle Verteilung von Exploit-Kits in Deutschland

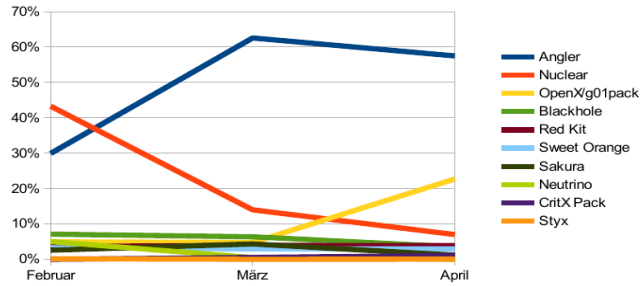


Abbildung 3: Top 10 Detektionen von Exploit-Kits in Deutschland in den Monaten Februar 2014 – April 2014 (Quelle BSI)

Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit:
Zweck

Lagebild
Cyber-Sicherheit

- Auslösen akuten Handlungsbedarfs
- Frühwarnung noch nicht betroffener Bereiche
- Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen
  - Welche Maßnahmen sind unverzichtbar?
  - Welche Maßnahmen sind wirtschaftlich?
- Basis für Risikoentscheidungen
  - Welches Risiko ist tragbar?
- Ableiten des präventiven/reaktiven Handlungsbedarfs
- Ableiten eines politischen Handlungsbedarfs

Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit:
Adressaten

Lagebild
Cyber-Sicherheit

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

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

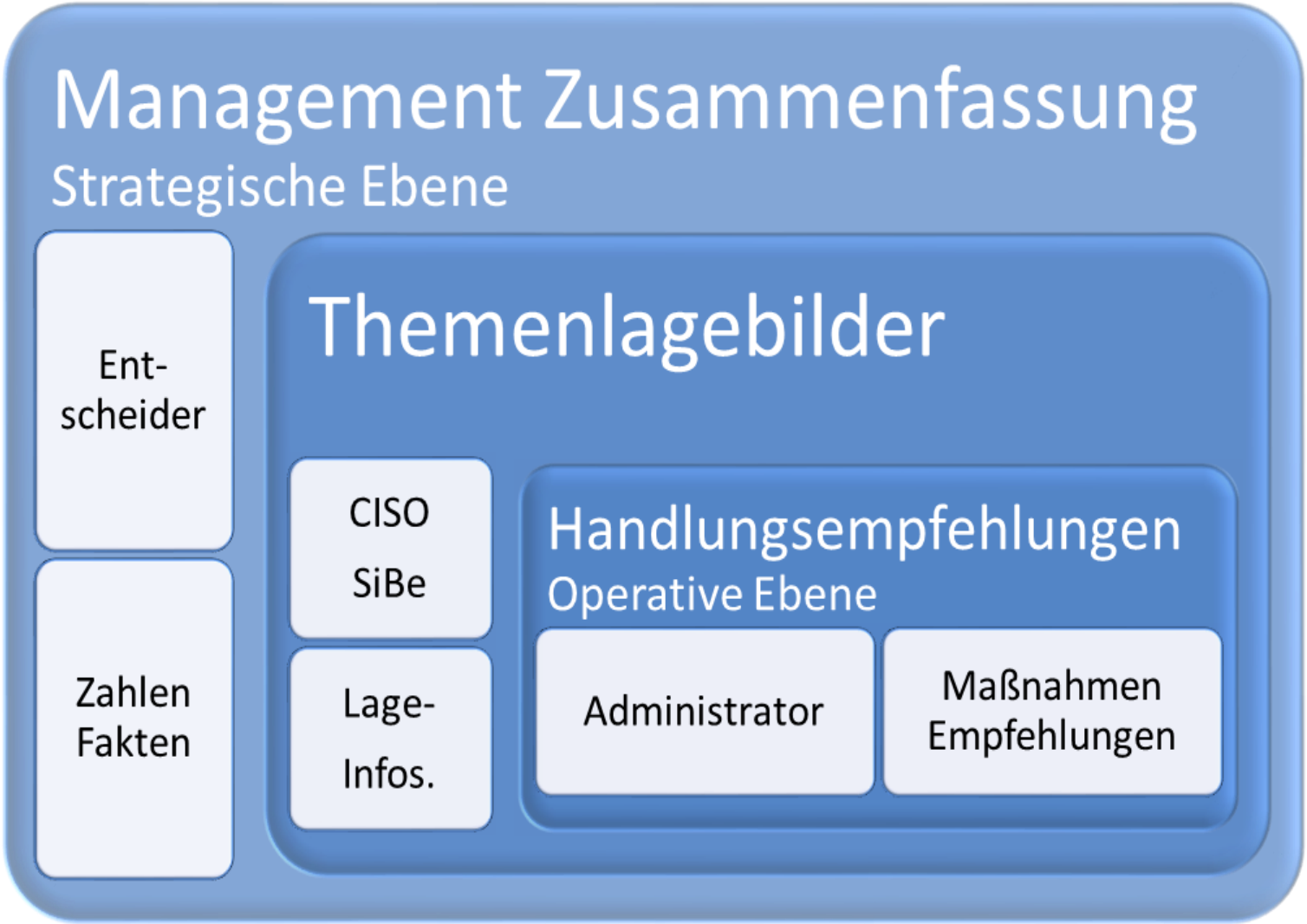
Institutionen, die **mittelbaren Einfluss** besitzen auf IT-Sicherheit:

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

Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit:
Zielgruppen - Hierarchieebenen -

Lagebild
Cyber-Sicherheit



Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit:
Quellen

Lagebild
Cyber-Sicherheit

Quellen des Bundes

- ✓Lagezentrum
- ✓Netze des Bundes
- ✓Meldestelle

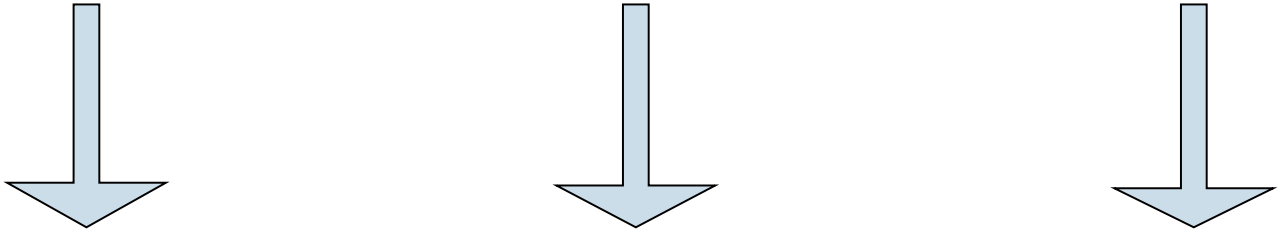
Quellen der Allianz

- ✓Partner der Allianz
- ✓gemeldete Vorfälle

Allianz für
Cyber-Sicherheit

Sonstige Quellen

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

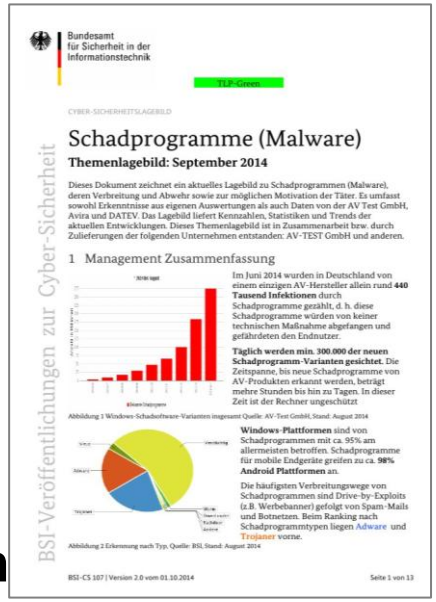


Lagebild Cyber-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit:
Themenlagebilder

Lagebild
Cyber-Sicherheit


Bundesamt
für Sicherheit in der
Informationstechnik

TLP-Green

CYBER-SICHERHEITSLAGEBILD

Schadprogramme (Malware)

Themenlagebild: September 2014

Dieses Dokument zeichnet ein aktuelles Lagebild zu Schadprogrammen (Malware), deren Verbreitung und Abwehr sowie zur möglichen Motivation der Täter. Es umfasst sowohl Erkenntnisse aus eigenen Auswertungen als auch Daten von der AV Test GmbH, Avira und DATEV. Das Lagebild liefert Kennzahlen, Statistiken und Trends der aktuellen Entwicklungen. Dieses Themenlagebild ist in Zusammenarbeit bzw. durch Zulieferungen der folgenden Unternehmen entstanden: AV-TEST GmbH und anderen.

1 Management Zusammenfassung

Im Juni 2014 wurden in Deutschland von einem einzigen AV-Hersteller allein rund **440 Tausend Infektionen** durch Schadprogramme gezählt, d. h. diese Schadprogramme würden von keiner technischen Maßnahme abgefangen und gefährdeten den Endnutzer.

Täglich werden min. 300.000 der neuen Schadprogramm-Varianten gesichtet. Die Zeitspanne, bis neue Schadprogramme von AV-Produkten erkannt werden, beträgt mehre Stunden bis hin zu Tagen. In dieser Zeit ist der Rechner ungeschützt

Abbildung 1 Windows-Schadsoftware-Varianten insgesamt Quelle: AV-Test GmbH, Stand: August 2014

Windows-Plattformen sind von Schadprogrammen mit ca. 95% am allermeisten betroffen. Schadprogramme für mobile Endgeräte greifen zu ca. **98% Android Plattformen** an.

Die häufigsten Verbreitungswege von Schadprogrammen sind Drive-by-Exploits (z.B. Werbebanner) gefolgt von Spam-Mails und Botnetzen. Beim Ranking nach Schadprogrammtypen liegen Adware und Trojaner vorne.

Abbildung 2 Erkennung nach Typ, Quelle: BSI, Stand: August 2014

BSI-CS 107 | Version 2.0 vom 01.10.2014

Seite 1 von 13

BSI-Veröffentlichungen zur 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**

Statistiken und Analysen zu Schwachstellen

Bundesamt
für Sicherheit in der
Informationstechnik

Schwachstellen
Lage / Daten / Fakten

Lagebild
Cyber-Sicherheit

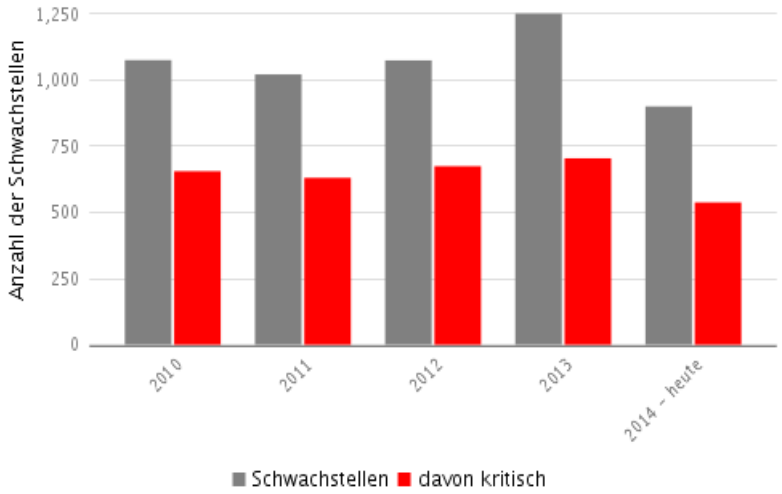


Abbildung: Anzahl aller Schwachstellen der betrachtete Softwareprodukte,
Quelle: BSI, Stand: September 2014

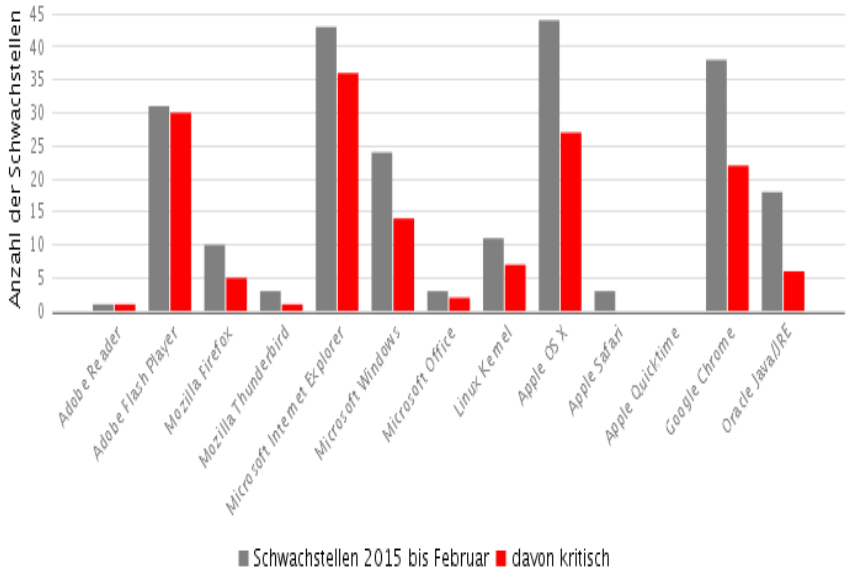


Abbildung:Anzahl aller entdeckten Schwachstellen bis Februar 2015, in den weitverbreiteten Softwareprodukten,
Quelle:BSI, Stand: Februar 2015

Täglich 2 neue kritische Schwachstellen

Mindestens 6% Windows XP-Clients

11% aller Benutzer arbeiten auf einem **ungepatchten Windows-Betriebssystem** (Win 7, Win 8, Windows Vista).

5,3% der Nutzer setzen **veraltete Systeme** ein, für die es keine Updates mehr gibt

Statistiken und Analysen zu Schadprogrammen (Malware)

Schadprogramme
Lage

- Die Gefährdung einer Infektion mit Schadprogrammen ist **sehr hoch**.

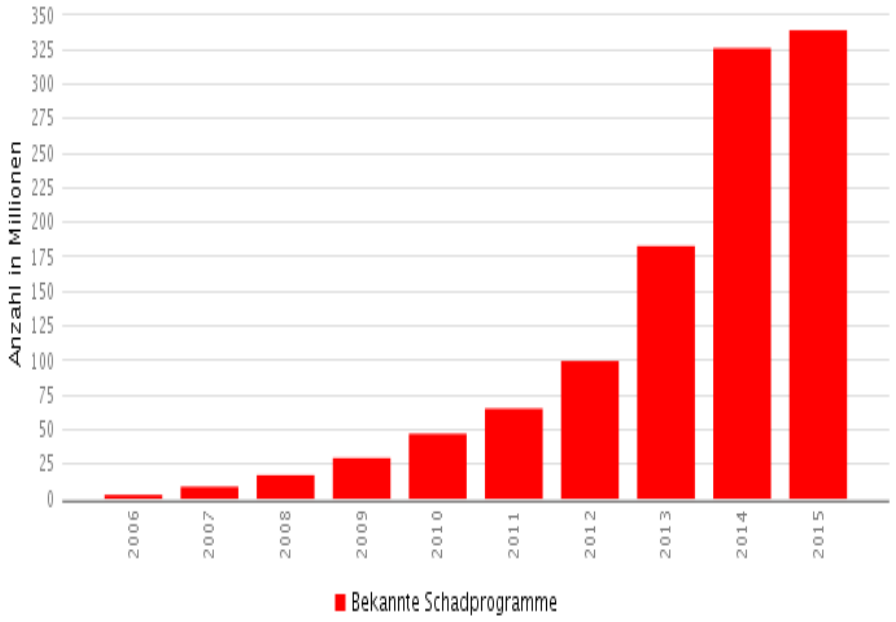
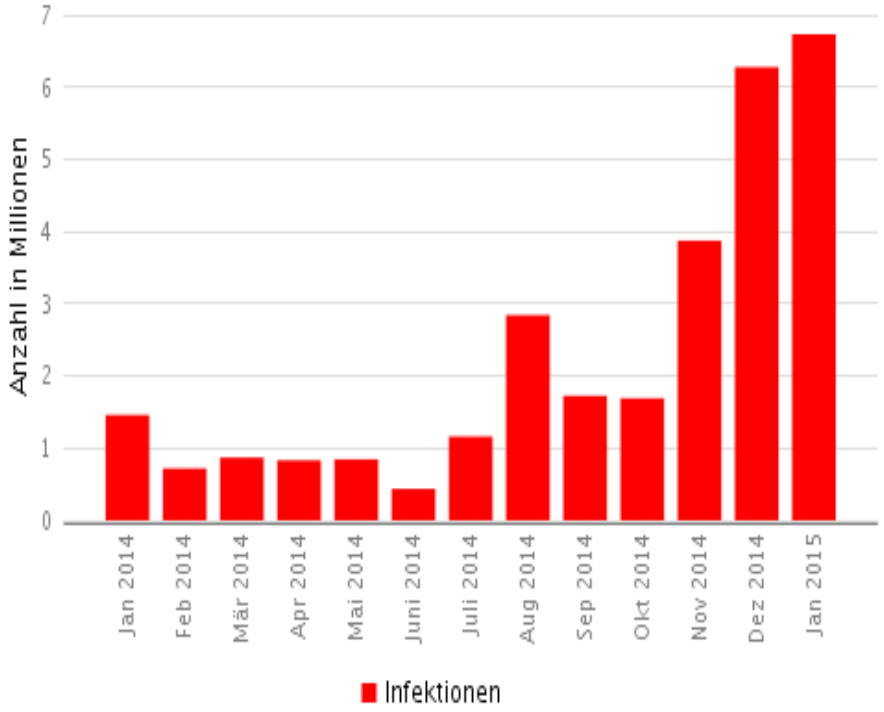


Abbildung: Windows-Schadsoftware-Varianten insgesamt Quelle: A V-Test GmbH, Stand: Januar 2015



Infektionen mit Schadsoftware in Deutschland, Quelle: ein AV Hersteller, Stand: Januar 2015

Bundesamt
für Sicherheit in der
Informationstechnik

Schadprogramme
Fakten

Lagebild
Cyber-Sicherheit

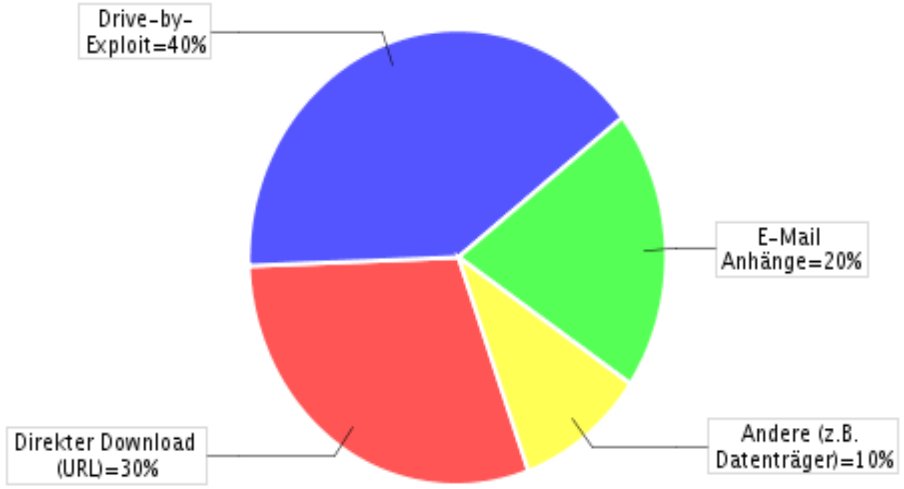
- Im Januar 2015 wurden in Deutschland von einem einzigen AV-Hersteller allein rund **6,7 Millionen Infektionen durch Schadprogramme** gezählt.
- **Täglich** werden **min. 300.000 neue Schadprogramm-Varianten** gesichtet.
- Die Zeitspanne, bis neue Schadprogramme von AV-Produkten erkannt werden, beträgt **mehre Stunden bis hin zu Tagen**.
- In dieser Zeit ist der Rechner ungeschützt.
- **Windows-Plattformen** sind von Schadprogrammen mit ca. **95%** am allermeisten betroffen.
- Neue Schadprogramme-Varianten für mobile Endgeräte greifen zu ca. **98% Android Plattformen** an und befinden sich fast ausschließlich außerhalb von Google Play.

Tägl. min. 300.000 neue Schadprogramm-Varianten
In den letzten 12 Monaten: **340.000.000 Malware** (**Windows**)

Schadprogramme
Erkannte Malware-Typen

- Die häufigsten **Verbreitungswege** von Schadprogrammen sind **Drive-by-Exploits** (z.B. Werbebanner) gefolgt von **Spam-Mails** und **Botnetzen**.

- Beim Ranking nach **Schadprogrammtypen** liegen **Trojaner** und **Adware** vorne.



Malware-Verbreitung über **Drive-By-Exploit**, **Download** und **E-Mail**

Schadprogramme
Mobile Endgeräte

Über **Apps** werden derzeit die **meisten** Schadprogramme auf **mobilen Endgeräte** verbreitet

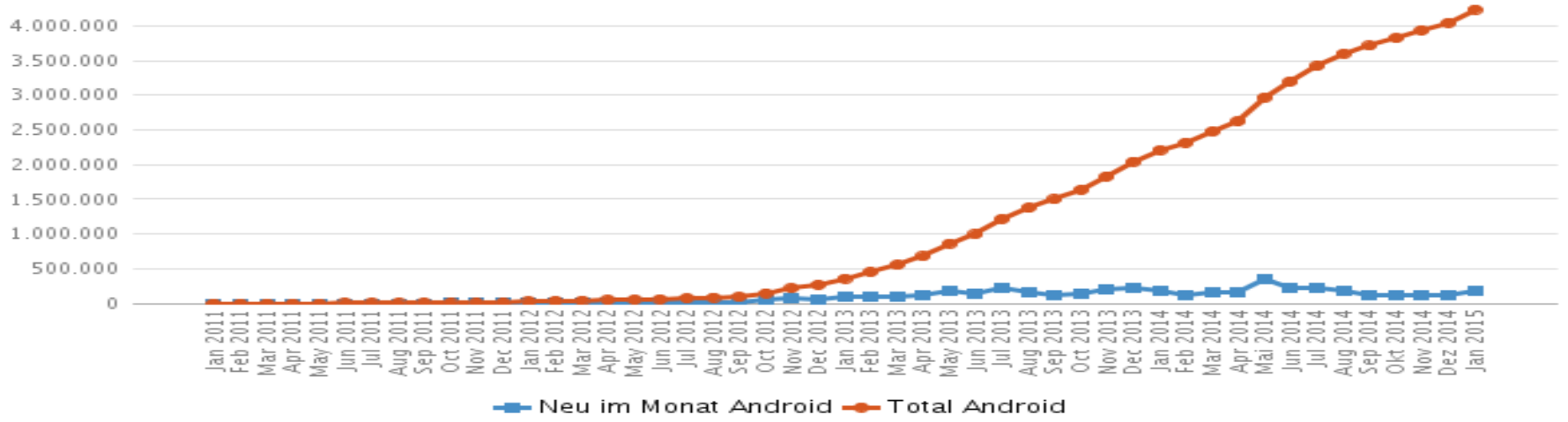


Abbildung: Anzahl schadhafter Android-Applikationen, Quelle: AV TEST GmbH, Stand: Januar 2015

Die blaue Linie ist hier die Anzahl neuer Varianten pro Monat, die rote Linie die Gesamtsumme aller bekannten Varianten schadhafter Android-Apps.

mehr als **4.200.000 verschied. mobile Malware** (**Android**)

andere mobile Plattformen (**Apple iOS, Windows Phone**)
nur **jeweils weniger als 10** gefährliche Apps bekannt

Statistiken und Analysen zu Exploit-Kits

Bundesamt
für Sicherheit in der
Informationstechnik

Schwachstellen: Exploit-Kits
Lage / Daten / Fakten

Lagebild
Cyber-Sicherheit

- **Häufigste Exploit-Kits** Detektionen in D:
  - Angler, Sweet Orange, Nuclear Exploit-Kit
  - Angler EK seit Monaten für 50 - 80% der Detektionen in D verantwortlich

- **Schwachstellen:**
  - 01.2015 / 02.2015: 3 0-Day-Schwachstellen in Adobe Flash Player
  - Verwendung im Angler sowie dem HanJuan Exploit-Kit bekannt.
    - Folge: u.a. Schadsoftware-Infektion (Bedep) mit Ziel Klickbetrug.
  - Anzeichen für Ausnutzung einer dieser Schwachstellen bereits in 12.2014 (2 Monate vor dem Sicherheitsupdate)

© Fa. Adobe

- **Bedrohungseinschätzung** nach Anwendungen:

Adobe Reader / Acrobat	↘
Adobe Flash	↑
Microsoft Internet Explorer	↑
Microsoft Silverlight	→
Oracle Java	↘

- **Gesamtbedrohung durch Exploit-Kits**
  - Lageänderung im Herbst 2014
  - Nutzung neuer Exploits
  - Nutzung 0-Day-Exploits
  - Angriffskampagnen mittels bekannter Webseiten

Häufung neuer Exploits in sehr kurzem Zeitraum sehr auffällig
Erhebliche Verschärfung der aktuellen Bedrohungslage

Statistiken und Analysen zu DDoS

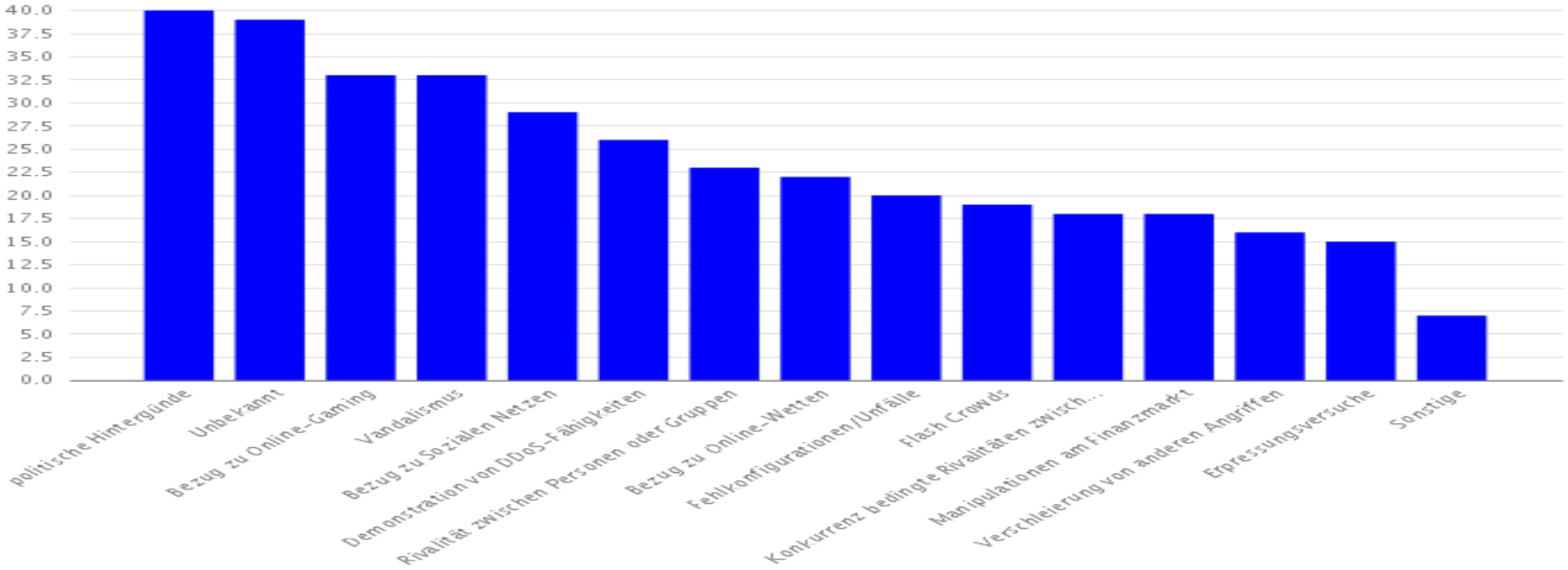
Bundesamt
für Sicherheit in der
Informationstechnik

DDoS
Lage / Daten / Fakten

Lagebild
Cyber-Sicherheit

- **Anzahl**
  - 01.-08.2014: ca 32.000 Angriffe in D, d.h. 133 Angriffe / Tag
- **Angriffsbandbreite:**
  - maximal beobachtet: 400 Gbps
  - Durchschnitt in D: 2,5 Gbps
  - Reduzierung gegenüber 2013
- **Angriffsmethoden**
  - Botnetz-Angriffe
  - Reflection Angriffe (DNS, NTP (rückläufig), CHARGEN, UDP-basiert)
- **Dauer / Durchschnittliche Dauer**
  - Wenige Minuten – mehrere Tage
  - Durchschnitt 30 Minuten
- **Kosten**
  - **Täter:** Rent a DdoS: 1 Stunde = 5 $, 1 Tag = 30-70 $
  - **Opfer:** in der Regel **deutlich höher** (direkte Kosten, akute Umsatzausfälle, langfristige Umsatzausfälle durch Kundenverlust Reputationsverlust)

DDoS
Tätermotivation



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

- **Häufig** ist die Motivation der Täter aber auch **nicht direkt ersichtlich**.

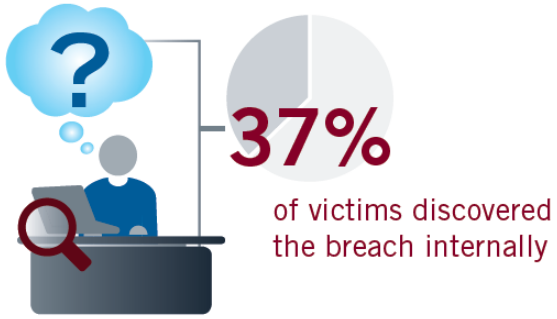
Statistiken und Analysen zu Advanced Persistent Threats (APT)

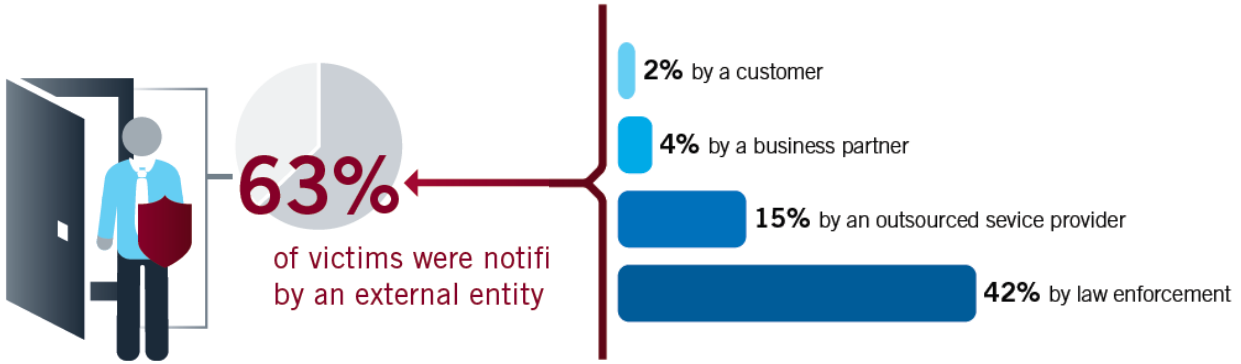
APT
Lage / Daten / Fakten

Gezielte Cyber-Spionage-Angriffe

- werden zu 2/3 extern entdeckt

- werden erst nach Monaten entdeckt





APT
Branchen / Angriffsmethoden

- Bevorzugte **Branchen**
  - Rüstungsindustrie
  - Hochtechnologiebranche: Auto, Schiffbau und Raumfahrt
  - Forschungseinrichtungen
  - Öffentliche Verwaltung

- Typische **Angriffsmethoden**
  - Vorbereitung: Social Engineering zu Zielpersonen
  - Angriffsvektor E-Mail mit Malware-Anhang an Zielperson
  - Angriffsvektor Watering-Hole-Angriff mit Malware auf Webseite

Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-Sicherheitslage:
Gesamtüberblick

Lagebild
Cyber-Sicherheit

Angriffsmittel

Ursachen → Wirkungen

Exploit-Kits nutzen vermehrt 0-day-Schwachst.

1,6% der Spam-Mails enthalten **Malware**

noch **6% Windows XP** im Einsatz (unsupportet)

Ca. **340 Mio. Schad-programme** für Windows

Ca. 1150 Botnetze weltweit, davon mehr als 1 Mio. Rechner in D

11% aller Nutzer: ungepatchte Systeme

tägl. 2 neue kritische Schwach-stellen in 13 wichtigen Produkten

DDoS-Angriffe:
Buy/rent a Bot:
30-70 $/Tag

O-day-Schwachst.
Deaktivierg
Adobe Flash

Drive-by-Exploits:
3% aller Webseiten in D verseucht

Hacktivismus zunehmend DDoS-Angriffe auf **KRITIS-Untern.**

56% der Unter-nehmen Ziel eines Angriffs

Aktuelle Bedrohung Schwach-stellen sehr hoch

Kosten nach DDoS-Attacke:
40T€ für KMU

Gezielte Cyber-spionage durch APT-Angriffe

133 DDoS-Angriffe pro Tag

Ca. 2500% Anstieg im letzten Jahr im **mobilen** Umfeld

Identitäts-diebstahl:
Clients:
16Mio/18Mio
eBay-Server:
145 Mio

Bundesamt
für Sicherheit in der
Informationstechnik

Lagebild Cyber-Sicherheit: Trend-Überblick / Gefährdungsbarometer

Lagebild
Cyber-Sicherheit

Bedrohungen	2012	2013	2014	Prognose
Denial of Service (DoS, DDoS)	→	→	↘	→
Botnetze	↗	→	→	→
Spam	→	↘	↗	→
Hacktivismus		→	→	→
Drive-by-Exploits	↗	↗	→	→
Schadprogramme	→	↗	↗	↗
Exploit-Kits		↗	→	↗
Identitätsdiebstahl	→	↗	↗	↗
Schwachstellen	→	↗	→	→
Advanced Persistent Threats (APT)		↗	→	↗

Gefährdungsbarometer ↗ steigend → gleichbleibend ↘ sinkend

OpenSource
vs
Proprietär-SW

Google (1)

Microsoft (2)

(3)

ORACLE (4)

im Spiegel des Lagebilds:

(5)

Die Cyber-Sicherheitslage aus der Sicht OpenSource und Proprietäre SW

(1) © Google: http://ladygaga.wikia.com/wiki/Google
(2) © Microsoft : http://www.thedrum.com/news/2014/04/30/microsoft-appoints-ipg-and-dentsu-aegis-handle-advertising-and-media-accounts-after
(3) © Apple : http://en.wikipedia.org/wiki/History_of_Apple_Inc.
(4) © Oracle: http://www.dataversity.net/one-big-data-acquisition-upend-entire-market/
(5) © Fa. Adobe: http://www.chip.de/news/Kritische-Luecke-in-Flash-Adobe-bietet-Notfall-Patch_66968598.html

Schadprogramme
Mobile Endgeräte

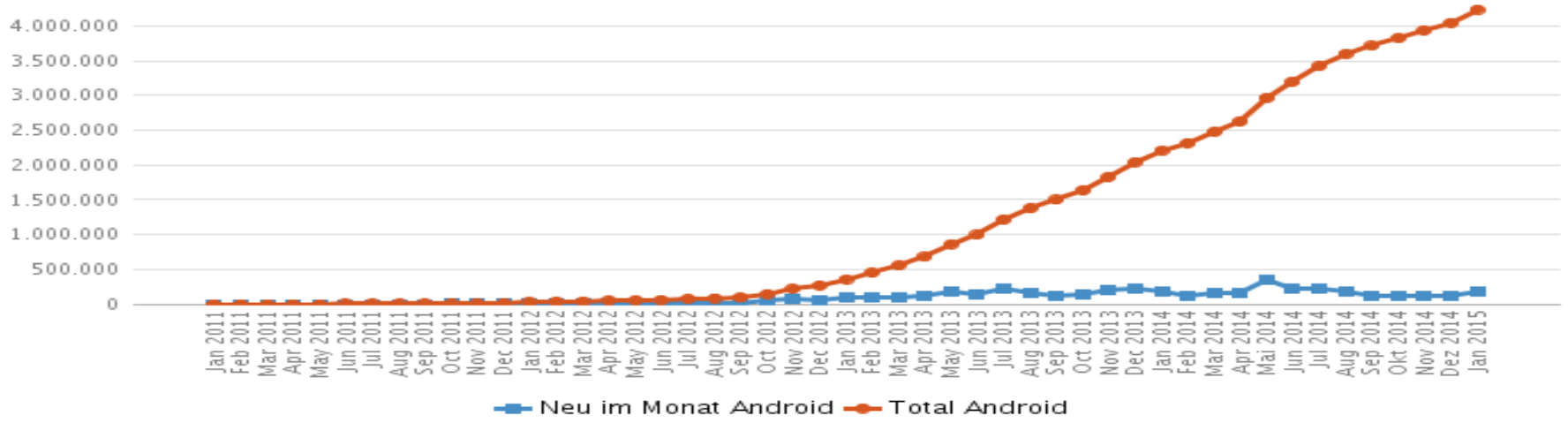


Abbildung: Anzahl schadhafter Android-Applikationen, Quelle: AV TEST GmbH, Stand: Januar 2015

Die blaue Linie ist hier die Anzahl neuer Varianten pro Monat, die rote Linie die Gesamtsumme aller bekannten Varianten schadhafter Android-Apps.

mehr als **4.200.000 verschied. mobile Malware** (**Android**) **(98%)**
in der Regel außerhalb des offiziellen App-Stores

andere mobile Plattformen (**Apple iOS, Windows Phone**)
nur **jeweils weniger als 10** gefährliche Apps bekannt

Schwachstellen

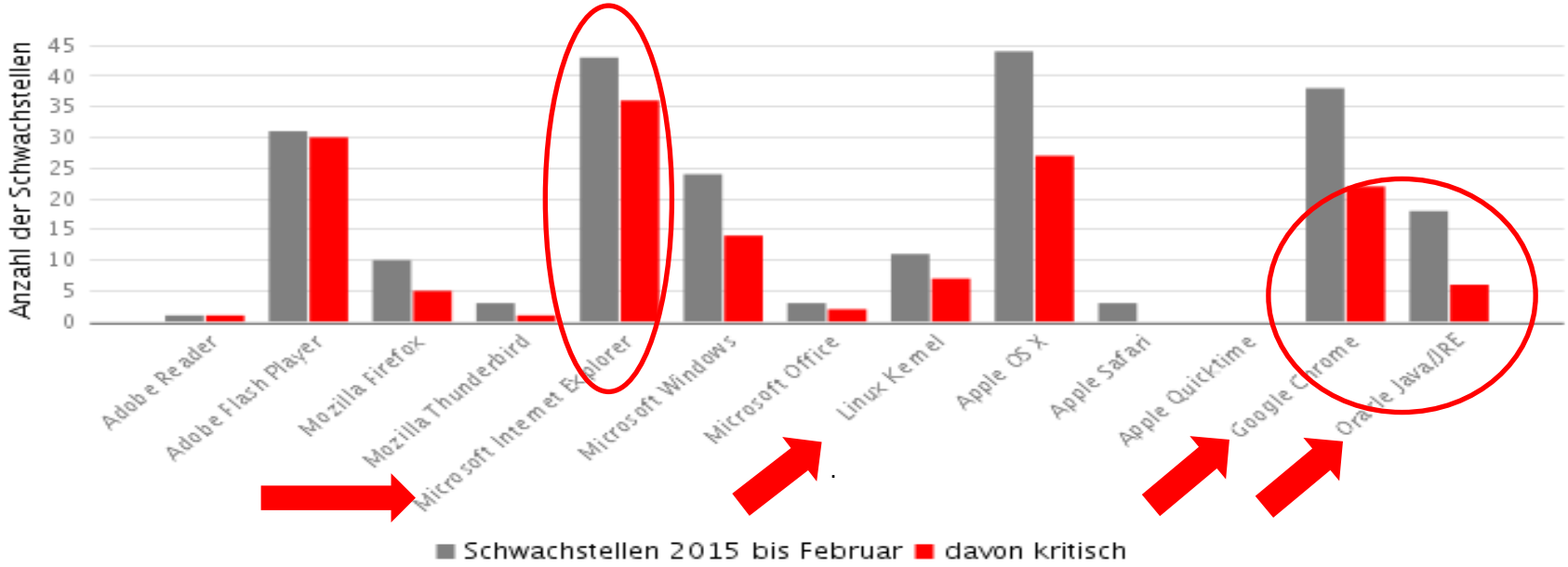


Abbildung:Anzahl aller entdeckten Schwachstellen Januar bis Februar 2015, in den weitverbreiteten Softwareprodukten,
Quelle:BSI, Stand: Februar 2015

Windows-Plattformen sind von Schadprogrammen mit ca. **95%** am allermeisten betroffen.

Proprietäre SW = Schwachstellenschleuder !?

MS-Schwachstellen, Java-Schwachstellen, Android, … vs.
Apple OS / iOS / Windows Phone, …
(unix-basierte, weiterentwickelte OS mit speziellen Erweiterungen)

Schwachstellen: Exploit-Kits

- **Schwachstellen:**
  - 01.2015 / 02.2015: 3 0-Day-Schwachstellen in Adobe Flash Player
  - Verwendung im Angler sowie dem HanJuan Exploit-Kit bekannt.
  - Anzeichen für Ausnutzung einer dieser Schwachstellen bereits in 12.2014

(1)

- **Bedrohungseinschätzung** nach Anwendungen:

Adobe Reader / Acrobat ™	↘
Adobe Flash ™	↑
Microsoft Internet Explorer ™	↑
Microsoft Silverlight ™	→
Oracle Java ™	↘

Exploit Kits: **vornehmlich Fokus auf Schwachstellen aus Proprietär- SW**
Führend: **MS Internet Explorer, Adobe Flash**

(1) © Fa. Adobe: http://www.chip.de/news/Kritische-Luecke-in-Flash-Adobe-bietet-Notfall-Patch_66968598.html

(7)

Google (1)

Microsoft (2)

(3)

ORACLE (4)

(5)

(6)

?

(1) © Google: http://ladygaga.wikia.com/wiki/Google
(2) © Microsoft : http://www.thedrum.com/news/2014/04/30/microsoft-appoints-ipg-and-dentsu-aegis-handle-advertising-and-media-accounts-after
(3) © Apple : http://en.wikipedia.org/wiki/History_of_Apple_Inc.
(4) © Oracle: http://www.dataversity.net/one-big-data-acquisition-upend-entire-market/
(5) © Fa. Adobe: http://www.chip.de/news/Kritische-Luecke-in-Flash-Adobe-bietet-Notfall-Patch_66968598.html
(6) http://www.openmagazine.org/tag/open-source/
(7) http://www.t5fixtures.com/t5-light-safety-guide/

Schwachstelle: Shellshock

(1)

- Shellshock ist (praktisch formuliert) eine **Server-Schwachstelle**, die sich von externen Angreifern nutzen lässt, um **Zugriff** auf eine **Bash/Kommandozeile** zu erhalten

- Betroffen waren eine Vielzahl von **Linux-Varianten**

Schwerwiegende Server-Schwachstelle in Linux

(1) http://www.heise.de/security/meldung/Bash-Luecke-ShellShock-ist-noch-nicht-ausgestanden-2403607.html

Implementierungsfehler: Heartbleed

- **OpenSSL** ist eine weitverbreitete Software-Bibliothek für die Absicherung von Web-Verkehr
- Die Heartbleed-Schwachstelle erlaubte das **Auslesen von Passwörtern** für die Webseite sowie der **privaten SSL-Schlüssel** der Webseite
- Betroffen waren Banken-Webseiten, Soziale Netzwerke, Web-Mailer, etc.
- Schwerwiegender **Implementierungsfehler**

OpenSSL
Cryptography and SSL/TLS Toolkit (1)

(2)

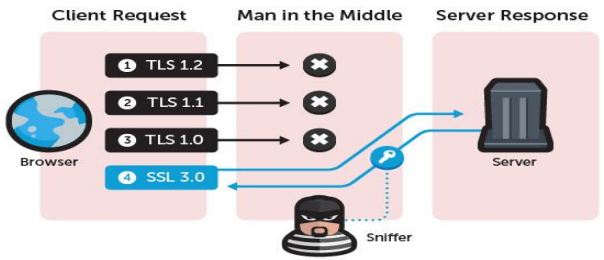
Schwerwiegende Implementierungsfehler in Open Source Produkt: nachträglich in Praxis entdeckt

(1) http://news.softpedia.com/news/New-OpenSSL-Fixes-Four-Security-Glitches-POODLE-Not-the-Biggest-Concern-462259.shtml
(2) http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/Heartbleed-does-not-kill-you-Just-yet/ba-p/6445806

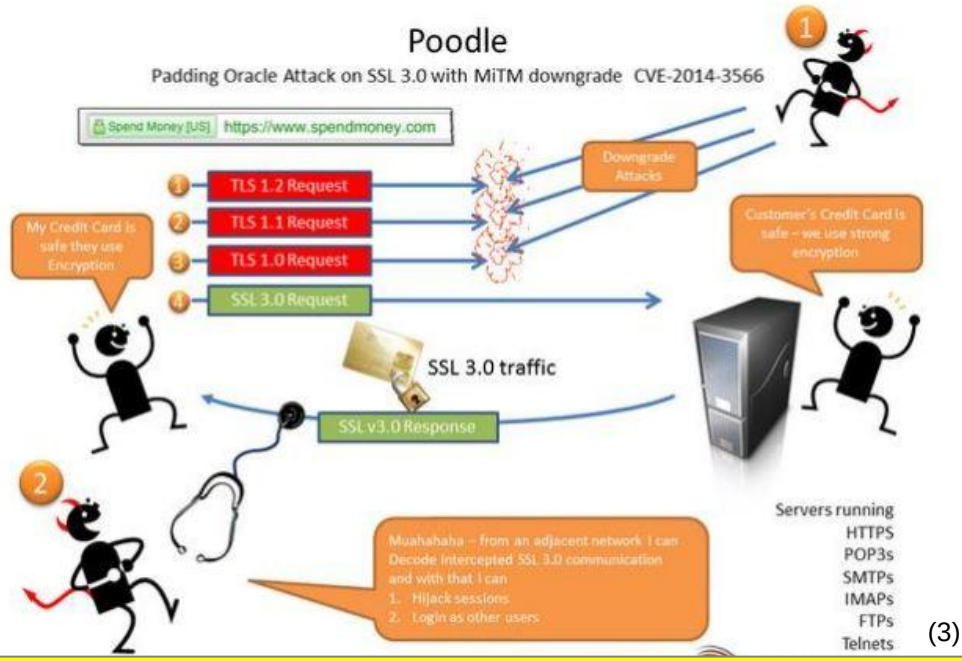
Implementierungsfehler: POODLE

(1)

- POODLE ist eine Schwachstelle, die es Angreifern erlaubt, **SSL/TLS-**Verbindungen auf das für MITM-Angriffe anfällige **SSL 3.0** zu downgraden
- Browser-Hersteller deaktivierten daraufhin die Unterstützung für SSL 3.0 in ihren Produkten
- Server-Betreiber forcierten den Einsatz von TLS 1.0



(2)



(3)

Schwerwiegende Implementierungsfehler in Open Source Produkt: nachträglich in Praxis entdeckt

(1): http://www.heise.de/security/meldung/Angriff-auf-Verschluesselung-Reaktionen-auf-die-Poodle-Luecke-2425244.html
(2) http://blog.trendmicro.de/unternehmen-und-user-schuetzen-sich-vor-poodle/
(3) https://modemworld.wordpress.com/2014/10/18/poodle-vulnerability-lab-issue-rc-viewer-with-browser-fix/

Ursachen / Hintergründe für Anfälligkeit

- **Zielobjekt:**
  - Grad der Fehlerrate / des Fehlerquotienten (z. B. infolge zunehmender Komplexität)
  - Verbreitungsgrad der SW (z. B. Einsatzbandbreite / Nutzung Android)
  - Zeitdauer des SW-Einsatzes
  - Patchverhalten / Patchstatus / Patchstand
    - Hersteller: Zeit zur Patcherstellung und Verbreitung
    - Nutzer: Umsetzung / Installation von Patches

- **Täter und Motivation**:
  - Kenntnisgrad über die SW / Zugriff auf Source Code (ggfs. Re-engineering) (Ablösung von ‚security-by-obscurity' / , Sicherheit durch Unklarheit')
  - Ausstattung der Angreifer (bessere Tools, monetäre Ausstattung, …)
  - Wirkungsgrad eines Cyberangriffs (monetäre Ziele, ‚Imagegewinn' des Hackers, …)

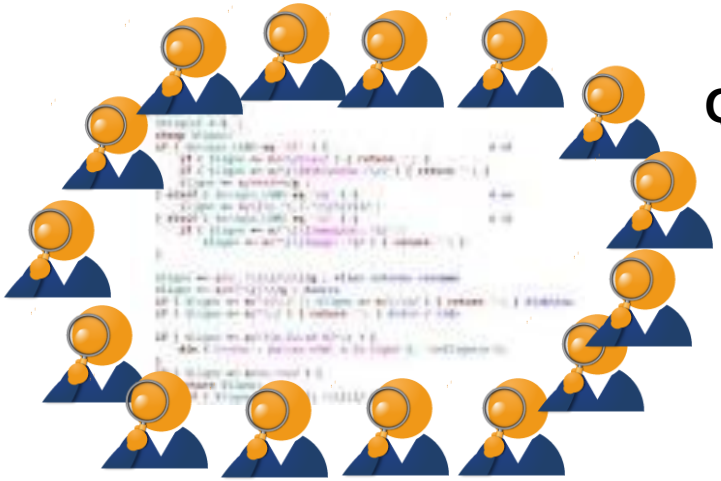
Erläuterung zu Ursachen

- **Komplexität**
  - **Wachsender Fehlerquotient** (Fehlerrate, Fehlerdichte, Fehlerhäufigkeit) infolge Komplexität und Programmgröße (Anzahl LoC) ($F = 4{,}04 + 0{,}0014\ LOC^{4/3}$ (ca. bis zu fünf Fehler pro 1000 Lines of Code))
  - **Implementierungsfehler:**
    - z.B. Kryptoalgorithmen (z. B: AES (Open Source)) sind in der Benutzung nicht automatisch sicher, da oft **fehlerhafte Implementierung** (s. auch Heartbleed, POODLE)

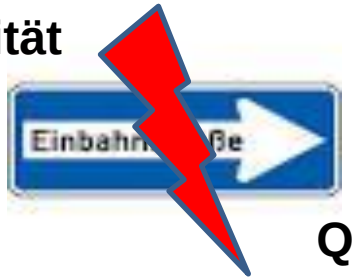
- **Usability/Benutzbarkeit/Anwendbarkeit** (z. B. GnuPG)

- **Verbreitungsgrad: Proprietäre Spezial-Betriebssysteme** sind
  - unbekannter (z. B. bei speziellen SCADA bzw. Industrie-IT)
  - Spezielle Programmiersprachen (spezielles Knowhow erforderlich)
  - Verbreitungsgrad gering
  - abgeschottet nach außen

Quantität ersetzt Qualität?



Quantität



Qualität

(1)

many eyes can‘t see straight =>

there is neither proof that open SW has fewer bugs (Whitfield Diffie)

Microsoft® .NET (2)

Initiative MS Development Framework

(1): http://www-01.ibm.com/software/integration/wmq/cc/
(2) http://www.clubic.com/lancer-le-telechargement-36366-0-microsoft-net-framework.html/

Bundesamt
für Sicherheit in der
Informationstechnik

Zusammenfassung

Lagebild
Cyber-Sicherheit

- Die Cybersicherheitslage in D ist **bedrohlich**!

- Deutschland
  - ist **massives Ziel** für Cyber-Crime
  - wird breit **cyber-ausspioniert**
  - ist Schwellenland für **Cyber-Sabotage**
  - die Dimension der Cyber-Angriffe auf Deutschland ist besorgniserregend
  - Praktisch **jedes Unternehmen wird cyber-attackiert**, nicht alle merken es

- Die Lage kann nur in **Zusammenarbeit** bewältigt werden

- Cybersicherheit und ‚OpenSource': **KEIN Automatismus,** aber
  OpenSource verträgt per se mehr Transparenz

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Lagebild
Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Klaus Keus
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