Hacking für Deutschland!? Aufgaben und Herausforderungen der Cyberabwehr im BSI

Andreas Könen
Vizepräsident, Bundesamt für Sicherheit in der Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

Hacking für Deutschland!? Aufgaben und Herausforderungen der Cyberabwehr im BSI

Andreas Könen
Vizepräsident, Bundesamt für Sicherheit in der Informationstechnik

Gefährdungslage

Wie bedroht ist Deutschlands Cyber-Raum?

Jede 40. Website ist infiziert

2015: Rund **drei Millionen Infektionen** mit Schadprogrammen pro Monat

Gezielte Cyber-Angriffe (Advanced Persistant Threats) werden im Schnitt nach **243 Tagen** entdeckt

2015: Bislang **639 kritische Schwachstellen** in Standard-Software

2015: Bislang ca. **420 Millionen** Schadprogramme für PCs

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

Bundesamt für Sicherheit in der Informationstechnik

Gefährdungslage

Cyber-Angriffe auf Unternehmen, Verwaltungen und Privatnutzer kommen **jeden Tag** vor.

Viele Angriffe verlaufen erfolgreich, weil die Angreifer

- professioneller werden,
- auf **Rahmenbedingungen** treffen, die sie zu ihrem Vorteil nutzen.

Digitalisierung und Vernetzung nimmt zu

- Beinahe alle Lebens- und Arbeitsbereiche sind erfasst ("always on"),
- Anforderungen an die Sicherheit von IT-Systemen, Applikationen und Software treten oft hinter ökonomischen und ergonomischen Randbedingungen zurück.

Ursachen
"Digitale Sorglosigkeit"

Erhöhte Sensibilität für das Thema IT-Sicherheit durch

- Enthüllungen rund um Snowden,
- die millionenfachen Identitätsdiebstähle 2014,
- Berichte über Cyber-Angriffe auf bekannte Unternehmen und Einrichtungen.

Im Gegenzug sieht man aber immer noch

- eine große Anzahl ungepatchter Systeme,
- unverschlüsselte Kommunikation,
- den Trend hin zu mobilen, immer erreichbaren Lösungen,
- verhältnismäßig geringe Investitionen in IT-Sicherheit.

Ursachen Schwachstellen

3 kritische Schwachstellen pro Tag!

Schwachstellen

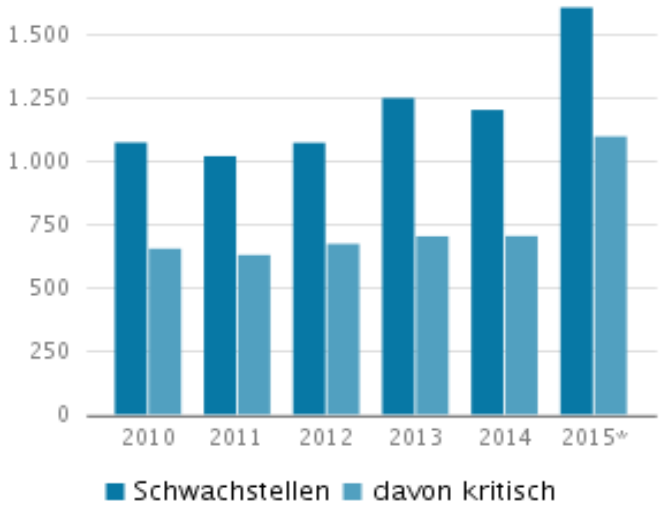


Abbildung: Anzahl aller Schwachstellen der gelisteten Softwareprodukte

*Die Werte für das Jahr 2015 wurden auf Basis der bis Ende Juli ermittelten Anzahl der Schwachstellen hochgerechnet

Softwareprodukte

Adobe Flash Player
Adobe Reader
Apple OS X
Google Chrome
Linux Kernel
Microsoft Internet Explorer
Microsoft Office
Microsoft Windows
Mozilla Firefox
Mozilla Thunderbird
Oracle Java/JRE

Tabelle: Ansicht von Softwareprodukten mit hoher Relevanz

Bundesamt für Sicherheit in der Informationstechnik

Angriffsmittel und -methoden
Evolution der Angriffe

		gezielte Angriffe Einzelziele
	zielgerichtete Angriffe selektierte Zielgruppe	
Flächenangriffe willkürliche Zielgruppe		
• **Verfügbarkeit** • **Sabotage** • **Betrug**	• **eSpionage** • **Sabotage** • **Identitätsdiebstahl**	• **Manipulation** • **Sabotage mit hohem Schadpotential** • **Informationsabfuhr**
• **2009 Conficker** • **2012 Dorifel**	• **2011 Bayer Server**	• **Advanced Persistent Threats** • **Stuxnet** • **TV5Monde**

Angriffsmittel und -methoden Advanced Persistent Threats (APT)

Typische Angriffsmethoden

- Vorbereitung: Social Engineering auf Zielperson
- Angriffsvektor E-Mail: Schadsoftware im Anhang, gerichtet an Zielperson
- Angriffsvektor Watering-Hole-Attack: Schadsoftware auf infizierter Webseite

Gezielte Cyber-Spionage Attacken

- werden in 2 von 3 Fällen erst von Externen aufgedeckt
- werden meist erst nach mehreren Monaten entdeckt

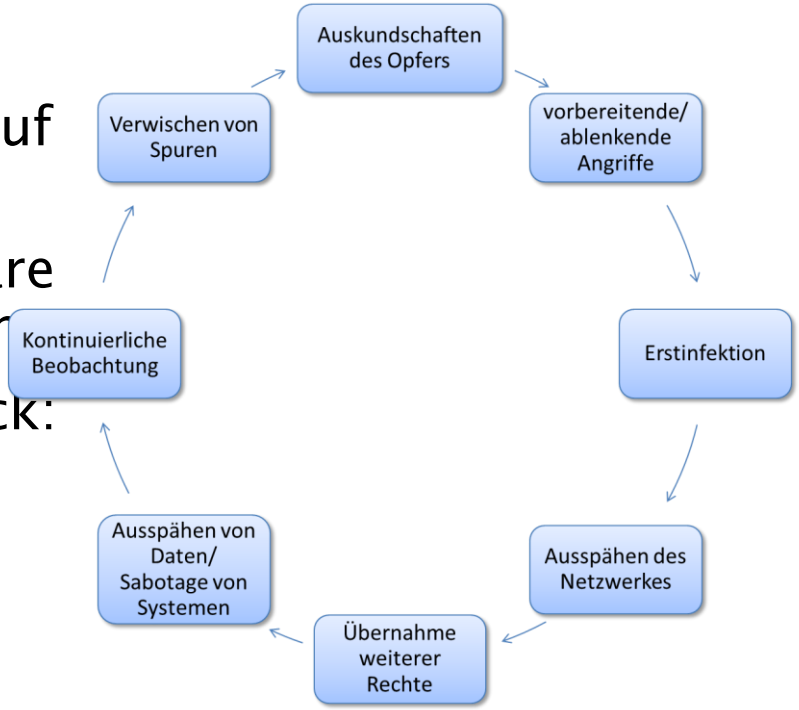


Abbildung: Vorgehensweise bei einem APT-Angriff

Angriffsmittel und -methoden Advanced Persistent Threats (APT)

- Zahl der Staaten mit offensiven Cyber-Aktivitäten nimmt zu (USA, UK, CHN, RU, Frankreich, Iran, Israel, Nordkorea, Pakistan, Indien, Syrien, …),
- APT-Angriffe werden als Dienstleistung angeboten,
- DAX-Unternehmen, KRITIS-Betreiber und KMU sind gleichermaßen von Cyber-Spionage und ggf. Sabotage betroffen,
- Prävention ist oftmals nicht möglich (technisch durch Zero-Days, menschlich durch Social Engineering),
- Risiko-Management: Rasche Detektion von Aktivitäten im eigenen Netz gewinnt an Bedeutung und kollidiert ggf. mit Datenschutz-Bedenken.

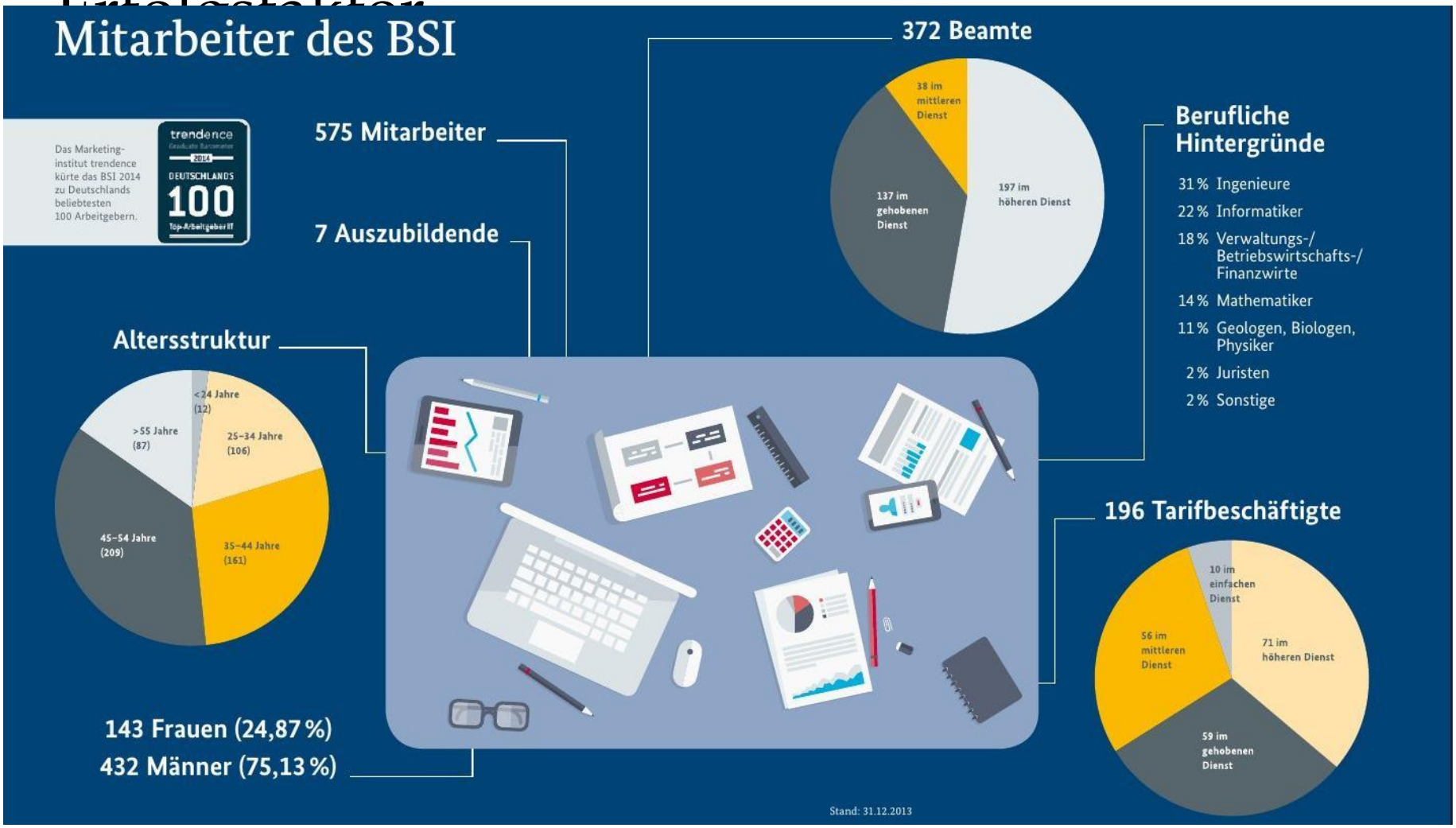
Beispiel: APT in einer Behörde

- Angreifer verleitet Empfänger einer E-Mail durch gutes Social Engineering zum Klicken des in der E-Mail enthaltenen Links,
- Dieser Link leitet das Opfer unerkannt zum Server des Angreifers (angezeigt wird die versprochene Webseite vom validen Webserver),
- Der Angriffsserver prüft automatisch das anfragende Opfersystem mittels JavaScript auf vorhandene Schwachstellen und nutzt diese dann aus (teilweise sogar mit ZeroDay-Exploits).

Beispiel: APT in einer Behörde

- Schadprogramm des Angreifers wird durch den Exploit auf das Opfersystem nachgeladen und ausgeführt,
- Angreifer ist nun in der Lage über das Internet auf das Opfersystem zuzugreifen und es fernzusteuern (Nachladen und Ausführen von weiteren Programmen, Suchen nach interessanten Dateien, etc.),
- Angreifer hat somit ersten Zugriff auf das interne Netzwerk und kann sich leicht auf weiteren Systemen Zugang verschaffen (im internen Netzwerk sind nur selten Schutzmechanismen implementiert, die diese Weiterverbreitung verhindern).

Der entscheidende Erfolgsfaktor



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Andreas Könen
Vizepräsident

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Tel.: +49 (0)228 99 - 9582 - 5210
Fax: +49 (0)228 99 - 10 - 9582 - 5210
andreas.koenen@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik