AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST

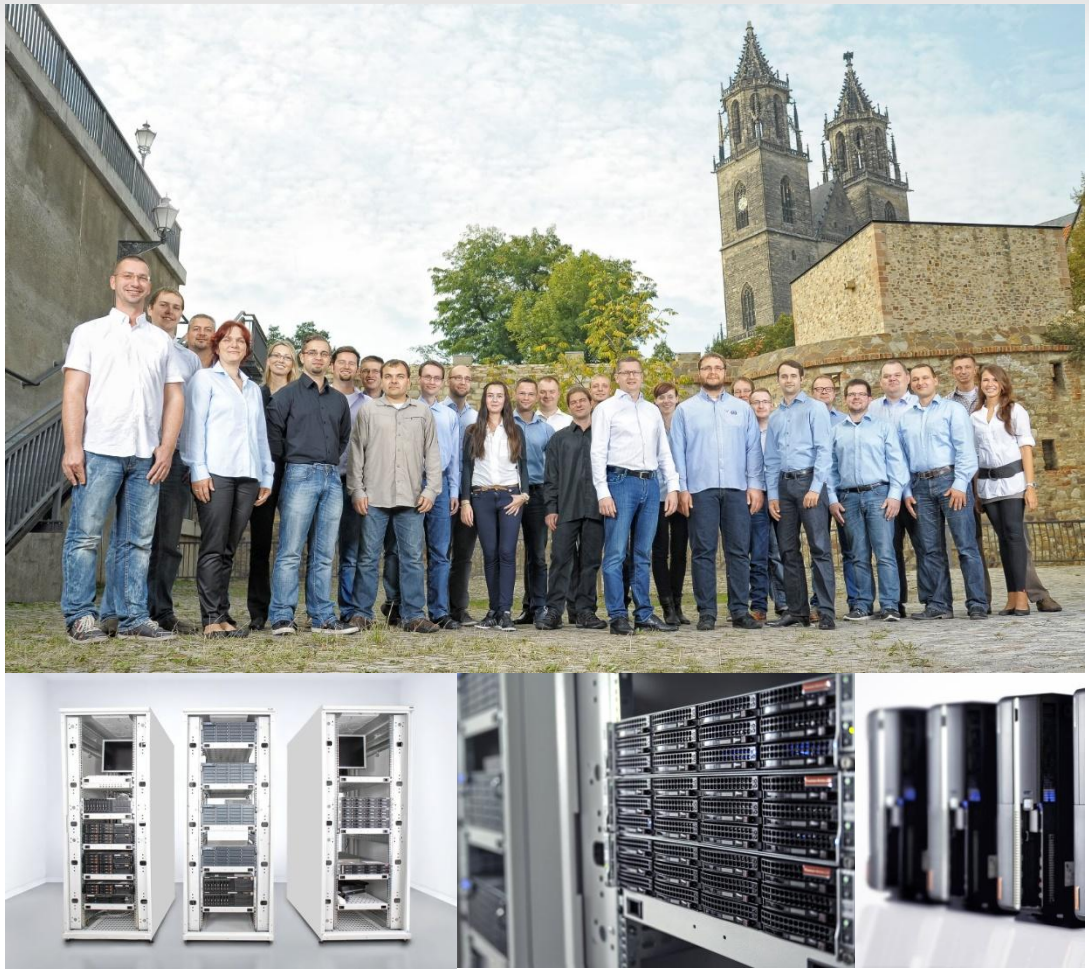
Sicherheitslage Android

SICHERHEITSLAGE ANDROID

- MEHR ALS 30 IT-SPEZIALISTEN
- MEHR ALS 15 JAHRE EXPERTISE IM BEREICH ANTIVIREN-FORSCHUNG
- UNTERNEHMENSGRÜNDUNG 2004

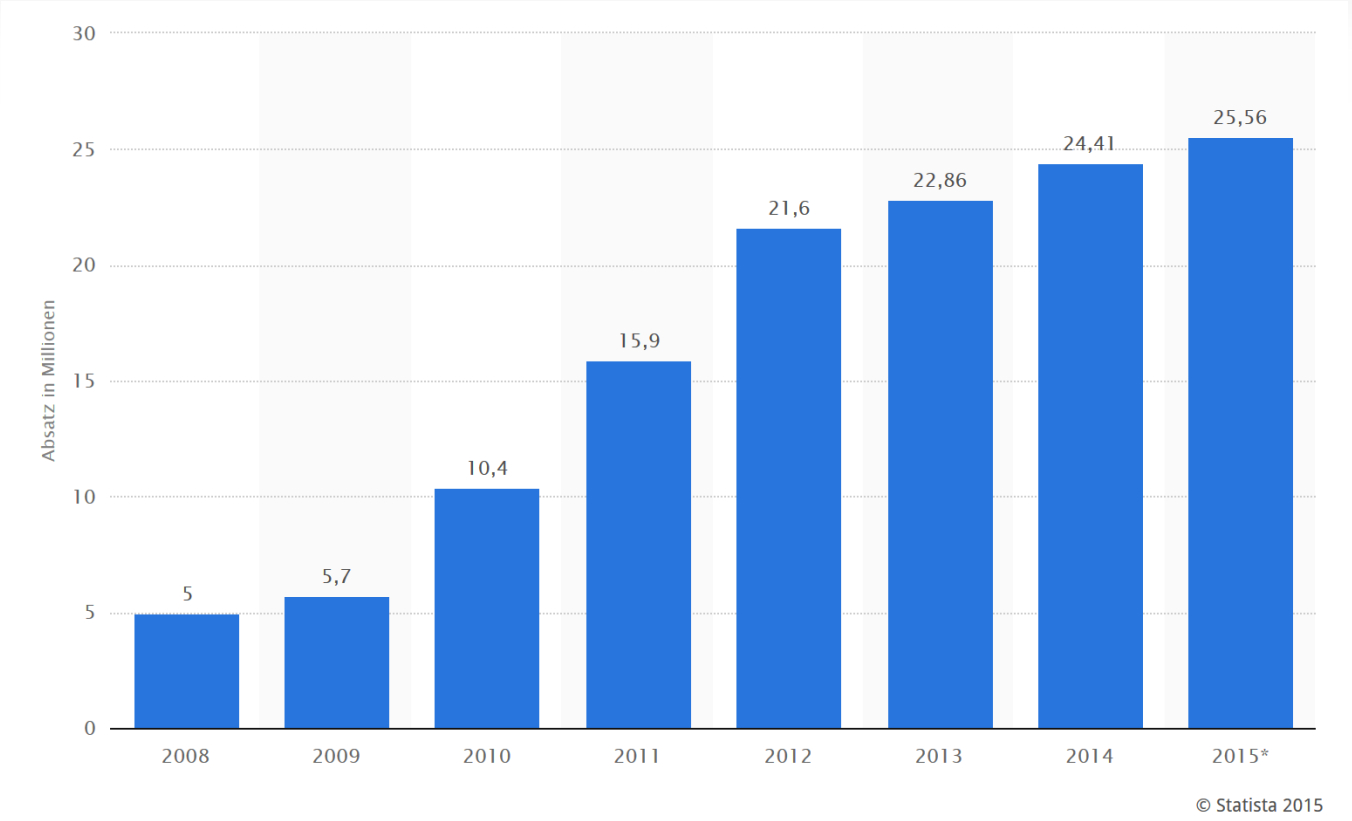
- **EINE DER GRÖßTEN VIREN-DATENBANK DER WELT**
- **400 CLIENT- UND SERVERSYSTEME**
- **1.000 TERABYTE TESTDATEN**
- **MEHR ALS 5.000 EINZEL- UND VERGLEICHSTESTS PRO JAHR**

- ANALYSE, TESTING, DEVELOPMENT, CONSULTING & SERVICES FÜR AV-HERSTELLER, FACHMAGAZINE, BEHÖRDEN & UNTERNEHMEN



SICHERHEITSLAGE ANDROID

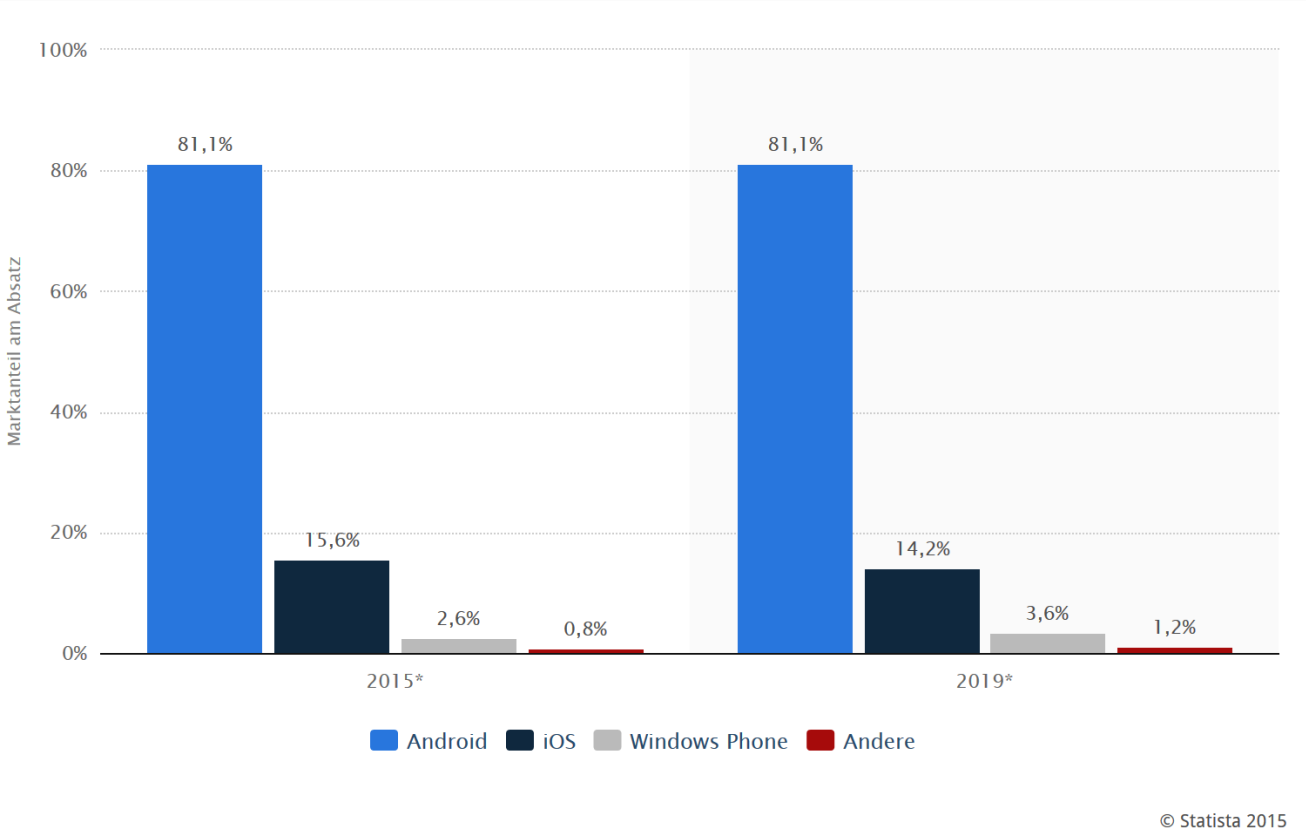
Über 25 Millionen neue Smartphones pro Jahr in Deutschland



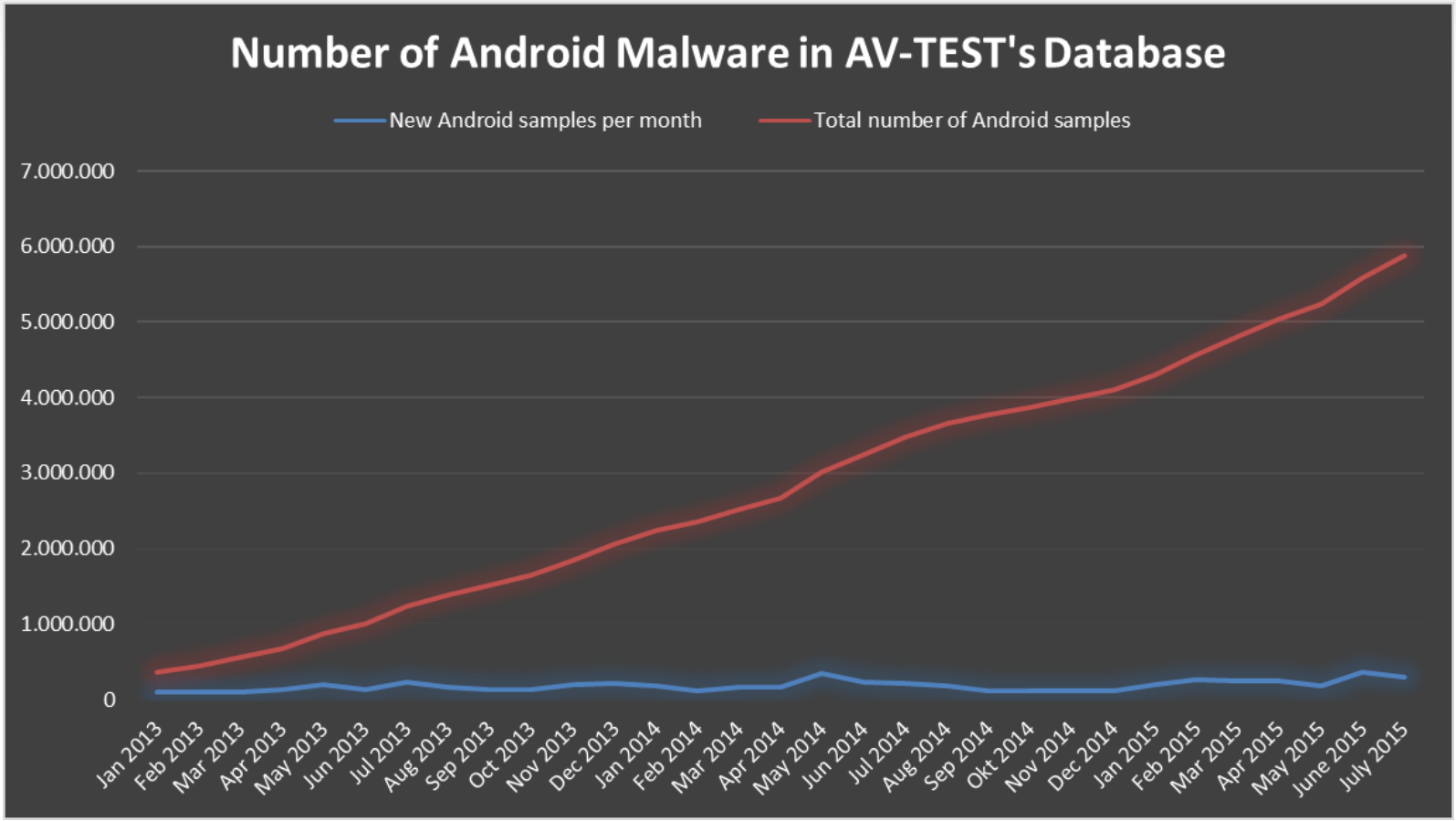
SICHERHEITSLAGE ANDROID

80% aller Smartphones in Deutschland sind Android-Geräte.

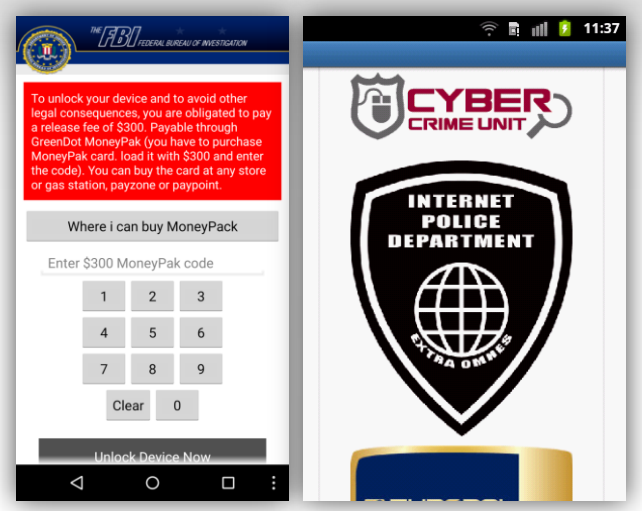
Und das wird wahrscheinlich auch so bleiben.



SICHERHEITSLAGE ANDROID



SICHERHEITSLAGE ANDROID



Ransomware

Banking Trojaner

Bitcoin Miner / Botnetze

Rootkits

Backdoors

Adware

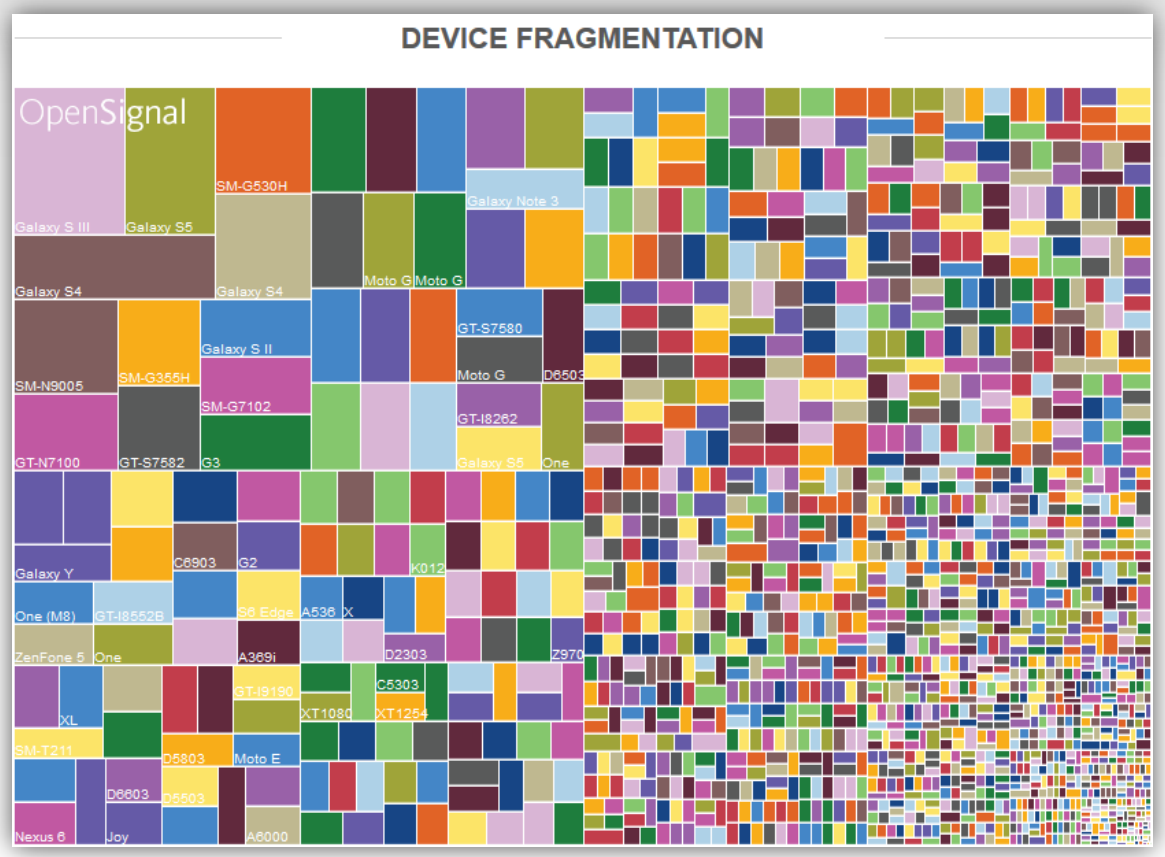
Spyware

Jeder Hersteller produziert dutzende Modelle

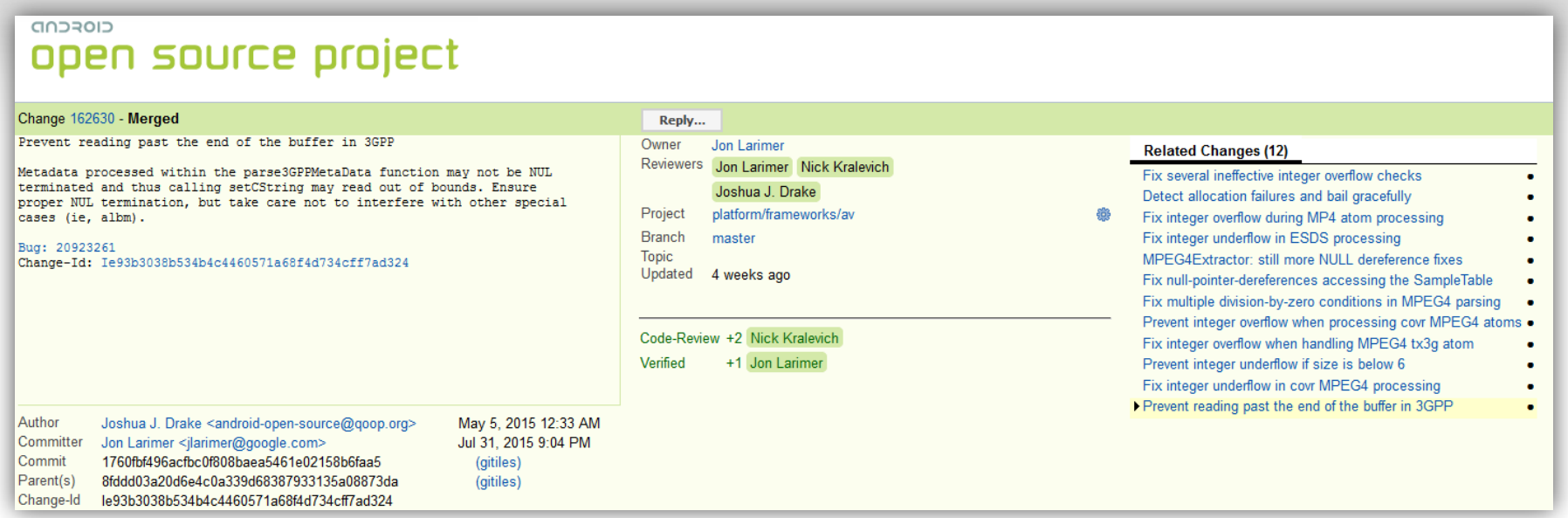
Für jedes Modell müssen Sicherheitsupdates entwickelt und getestet werden

Mobilfunkprovider müssen die Updates an Kunden verteilen

Nur die Top-Geräte erhalten Update-Support!



Quelle: http://opensignal.com/reports/2015/08/android-fragmentation/

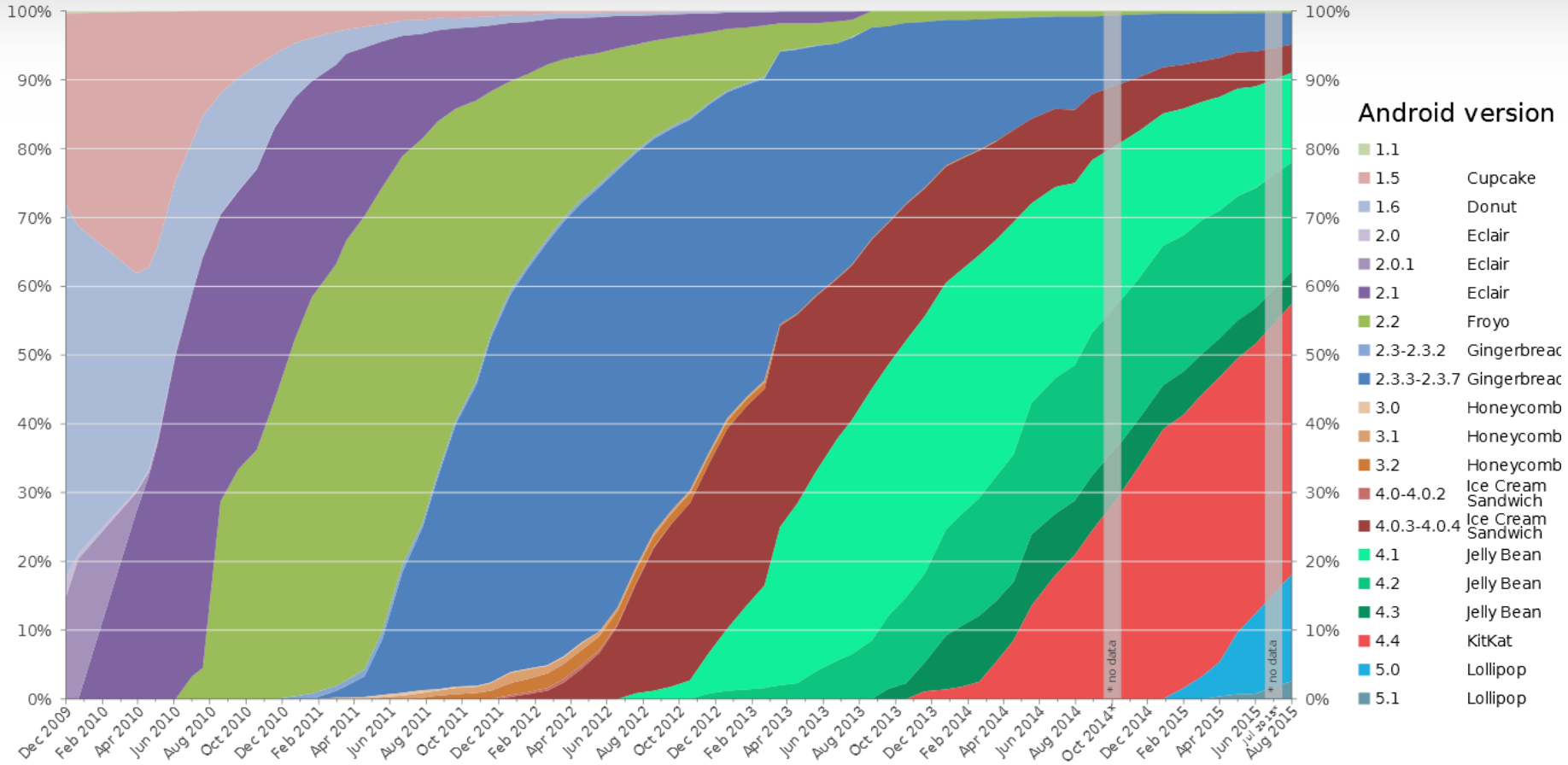


Android ist Open Source

Änderungen am Code (Bug Fixes) sind öffentlich nachvollziehbar

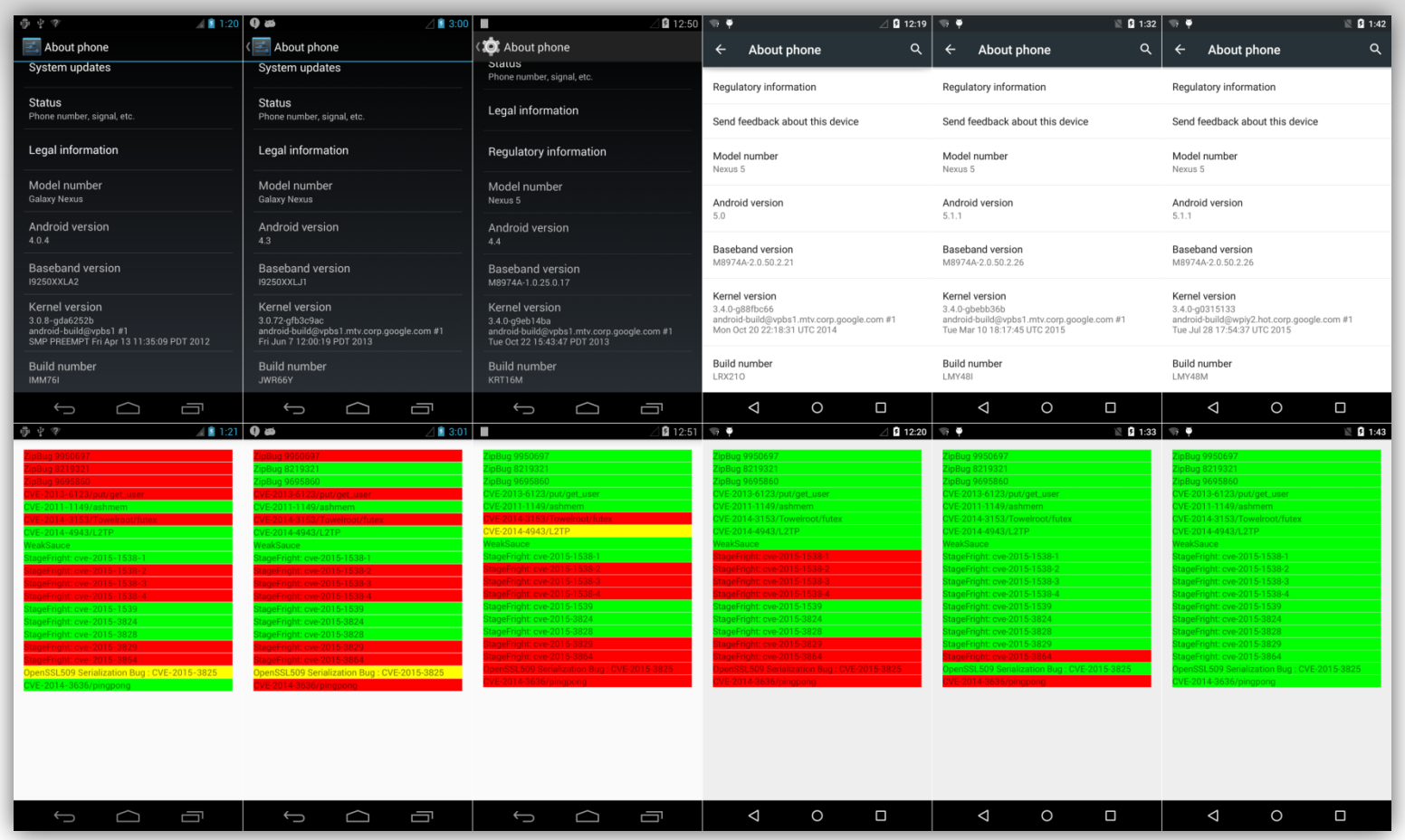
Exploits für geschlossene Sicherheitslücken können rückwirkend entwickelt werden

SICHERHEITSLAGE ANDROID



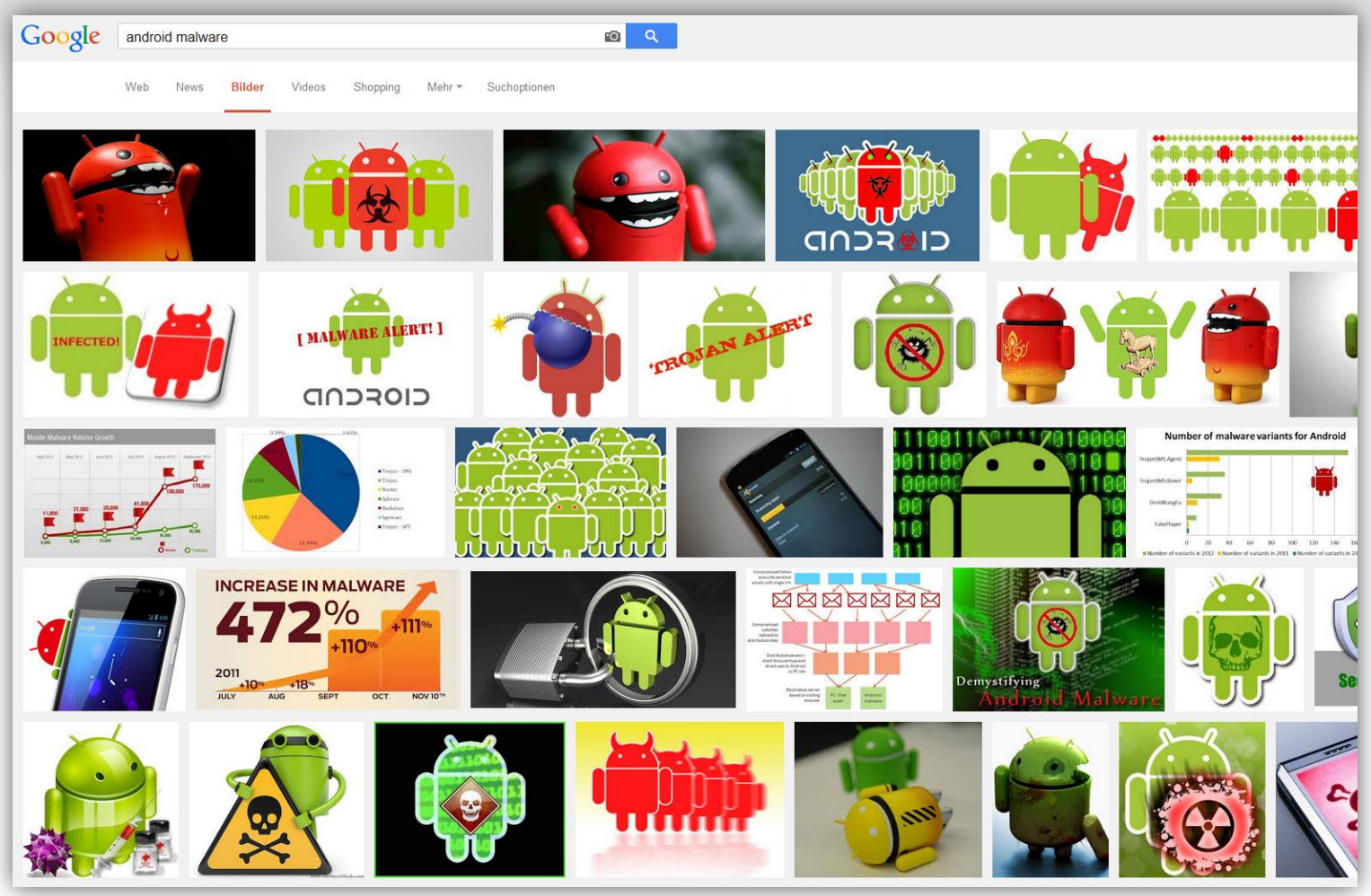
Quelle: https://en.wikipedia.org/wiki/Android_version_history

SICHERHEITSLAGE ANDROID



Android Vulnerability Test Suite: https://github.com/nowsecure/android-vts

SICHERHEITSLÜCKEN



Eine Sicherheitslücke in der Multimedia-Bibliothek von Android erlaubt Zugriff auf Mikrofon, Kamera, Bluetooth und Internet

Über Webseiten, Nachrichten und Werbeanzeigen kann die Lücke ausgenutzt werden

Angreifer können per MMS Malware auf einem Zielgerät installieren, ohne dass der Nutzer es merkt

Angreifer können manipulierte Werbung schalten, um eine große Menge an Endgeräten mit Schadsoftware zu infizieren

Quelle: https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

Experts Found a Unicorn in the Heart of Android

By Z Team

Monday, Jul 27 2015 at **13:02**

Share 10.4K Tweet 4543 Like 165 G+1 84 Share 182 Email 233 Share 31K

The Latest on Stagefright: CVE-2015-1538 Exploit is Now Available for Testing Purposes

By zLabs

Wednesday, Sep 9 2015 at **08:05**

Share 910 Tweet 1850 Like 1.1k G+1 73 Share 36 Email 91 Share 5818

Certifi-gate: Hundreds of Millions of Android Devices Could Be Pwned

by Check Point Research Team posted 2015/08/06

Certifi-Gate ist ein Angriff auf Mobile Remote Support Tools

Gerätehersteller stellen Systemschnittstellen für solche Tools zur Verfügung

Die Tools werden unzureichend vom System authentifiziert

Malware kann die Schnittstellen nutzen und das Gerät fernsteuern

Certifi-gate Found in the Wild on Google Play

by Check Point Research Team posted 2015/08/25

Quelle: https://www.blackhat.com/docs/us-15/materials/us-15-Bobrov-Certifi-Gate-Front-Door-Access-To-Pwning-Millions-Of-Androids.pdf

Samsung Keyboard Security Risk Disclosed:

Over 600M+ Devices Worldwide Impacted

Eine vorinstallierte Tastatur sucht automatisch nach Updates und benutzt eine ungesicherte Verbindung

Die runtergeladenen Updates werden unzureichend verifiziert

Ein Angreifer kann infizierte Updates verbreiten und damit
Sensoren auslesen (GPS, Kamera, Mikrofon)
Malware installieren
und Daten auslesen oder manipulieren

Quelle: https://www.nowsecure.com/keyboard-vulnerability/

Neben den Sicherheitslücken im Betriebssystem gibt es auch jede Menge Lücken in den eingesetzten Apps

Unsichere Apps betreffen auch andere Systeme wie iOS, Windows Phone und BlackBerry

Quelle: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

Neben Schadsoftware hat Android ein massives Problem mit Sicherheitslücken

Die Verteilung von Sicherheitsupdates dauert zu lange

Endbenutzer haben nur wenige Möglichkeiten, sich mit Sicherheitsupdates zu schützen

Unsichere Apps gibt es für alle Smartphone Plattformen

Welche Schutzmaßnahmen gibt es?

Mobile Security Apps

Mobile Device Management

Sicherheitsbewusstsein und Mitarbeiterschulung

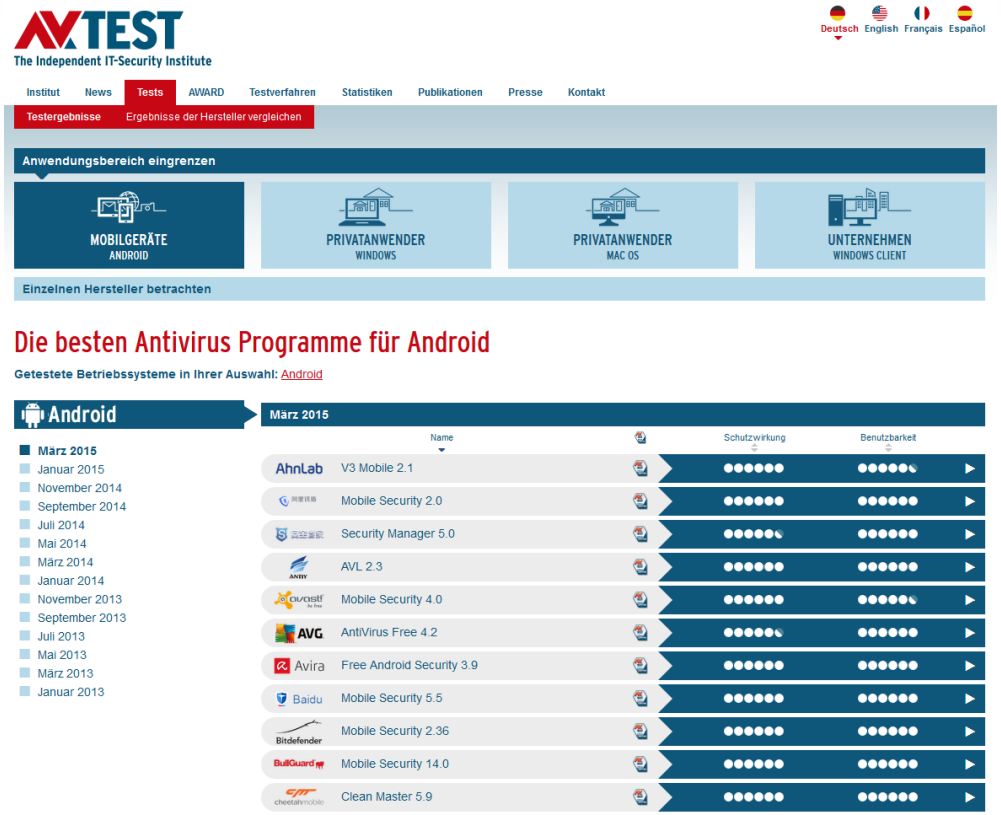
Allgemeine Verhaltensweisen

Mobile Security Apps

Testergebnisse auf www.av-test.de

Wichtige Funktionen:

- **Anti-Virus**
- **Anti-Diebstahl**
- **Browserschutz**



ZUSAMMENFASSUNG & SICHERHEITSTIPPS

- DIE AV-TEST QUALITÄSSIEGEL „CERTIFIED“ UND „APPROVED“
- 1.270 VERGEBENE AV-TEST ZERTIFIKATE SEIT 2010

- AUSGEZEICHNET WERDEN DIE JAHRESBESTEN SCHUTZLÖSUNGEN FÜR DIE BEREICHE HEIMANWENDER, UNTERNEHMEN UND MOBILE SECURITY.
- DER AV-TEST INNOVATION AWARD FÜR INNOVATIVE IT-SCHUTZLÖSUNGEN

Mobile Device Management

Verwaltung aller Mobilgeräte im Unternehmen

Sicherheitsrichtlinien können Nutzerverhalten einschränken

Individuelle App Stores ermöglichen eine qualifizierte Vorauswahl

Unternehmensdaten werden von persönlichen Daten getrennt

Sicherheitsbewusstsein und Mitarbeiterschulung

Integrieren Sie IT-Sicherheit in betriebliche Unterweisungen

Zur Orientierung hilft der IT-Grundschutz-Katalog des BSI

www.bsi.bund.de

Allgemeine Verhaltensweisen

Sperren Sie Ihre Geräte mit einem Lockscreen mit PIN- oder Passwort-Eingabe

Aktivieren Sie die Geräteverschlüsselung, sofern vorhanden

Benutzen Sie sichere und verschiedene Passwörter in allen Konten

Nutzen Sie Ihr Smartphone zur 2-Faktor-Authentifizierung, um Online-Konten zu schützen

Allgemeine Verhaltensweisen

Installieren Sie regelmäßig verfügbare Sicherheitsupdates

Achten Sie auf verschlüsselte Datenverbindungen (SSL & VPN)

Erstellen Sie regelmäßig Backups Ihrer Daten

“Rooten” Sie Ihr Gerät nicht

Proben Sie den Ernstfall: Was muss ich tun, wenn …?

Folgen Sie uns auf Twitter @avtestde

Finden Sie uns auf facebook.com/avtestorg

Aktuelle Test-Ergebnisse: www.av-test.de

Vielen Dank für Ihre Aufmerksamkeit!
Haben Sie noch Fragen?