

Der Smart-TV als Eingangstor ins Unternehmensnetzwerk

Hacking Day 2015

09. September 2015

www.oneconsult.com



Übersicht

- ▶ Advanced Persistent Threat (APT)
- ▶ Was sind «Smart-TVs»?
- ▶ Angriffe mit Smart-TVs
- ▶ Bestehende Angriffe
- ▶ Unser Angriff
 - ▷ Demonstration
 - ▷ Flash Exploit
 - ▷ Auswirkungen & Möglichkeiten
- ▶ Fazit

Advanced Persistent Threat

- ▶ 4 Phasen
 - ▷ Vorbereitung
 - ▷ **Infektion**
 - ▷ Verteilung
 - ▷ Persistenz



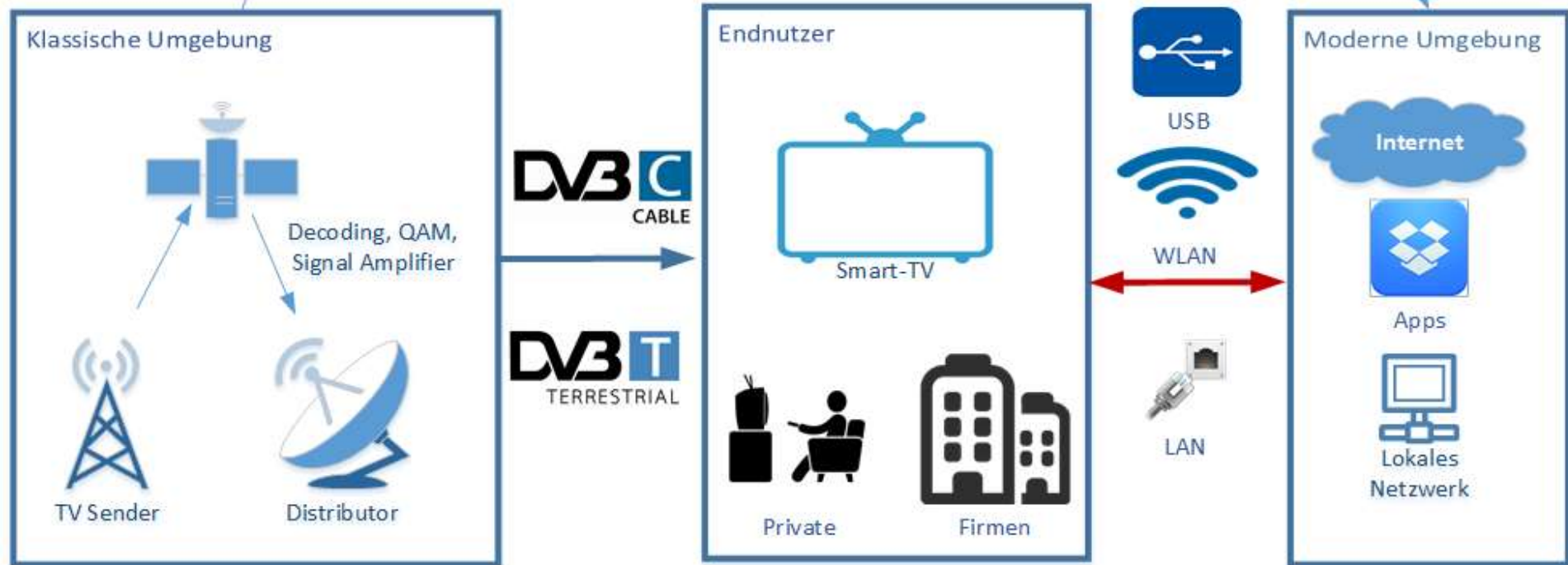


Angriffe mit Smart-TVs

- ▶ Informationsabfluss
 - ▷ Kamera / Mikrofone
 - ▷ USB Sticks
 - ▷ Angezeigte Inhalte (z.B. Präsentationen)
- ▶ Netzwerkzugang
 - ▷ Netzwerkangriffe
 - ▷ Ausgangspunkt für weitere Angriffe
- ▶ Informationsmanipulation
- ▶ **Angreifer ist persistent auf Smart-TV**
 - ▷ Physikalisch im Zielgebiet
- ▶ Bot-Net erstellen

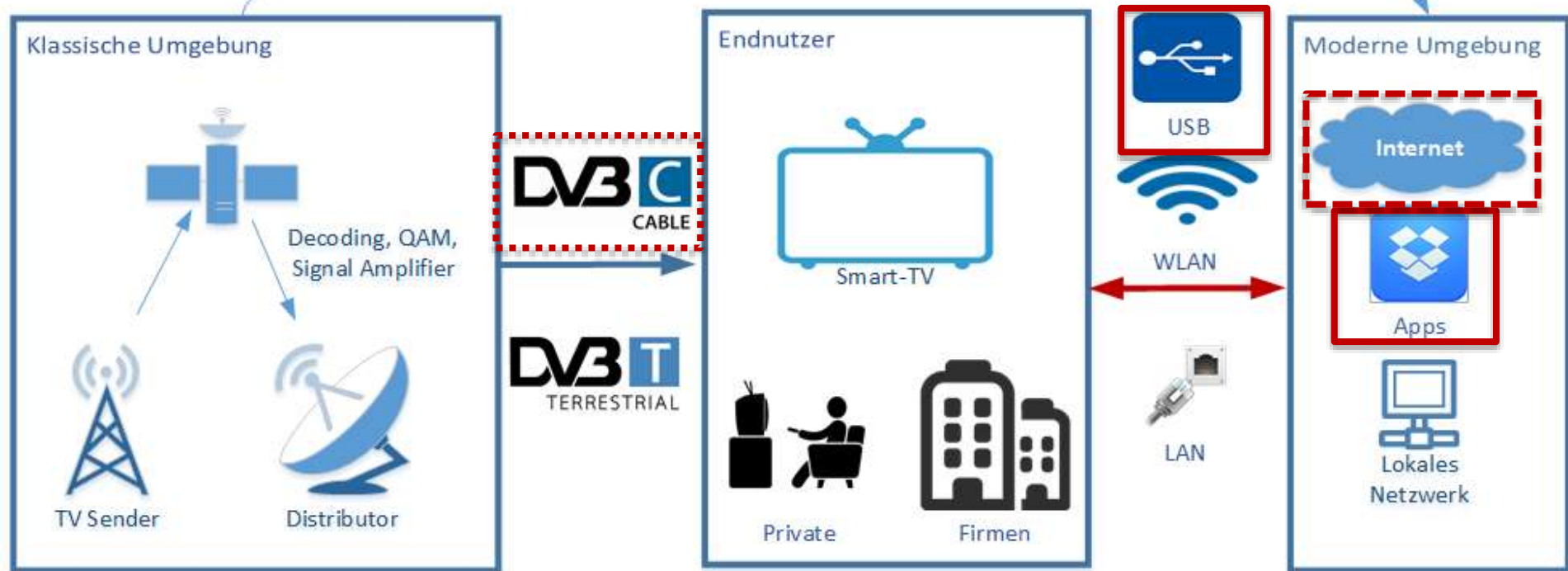


Moderne TV-Umgebung





Bestehende Angriffe





Bestehende Angriffe

- ▶ Generell
 - ▷ Sehr gute «Post Exploitation»
- ▶ USB
 - ▷ Physikalischer Zugriff benötigt
- ▶ DVB
 - ▷ Missbrauch integrierter Update-Funktion
 - ▷ (Noch) keine publizierten Decoder Exploits
- ▶ Apps
 - ▷ Manueller Download notwendig
- ▶ Internet
 - ▷ Manueller Download eines Files / Videos notwendig
 - ▷ Keine publizierten Angriffe auf das neue Samsung OS über das Internet

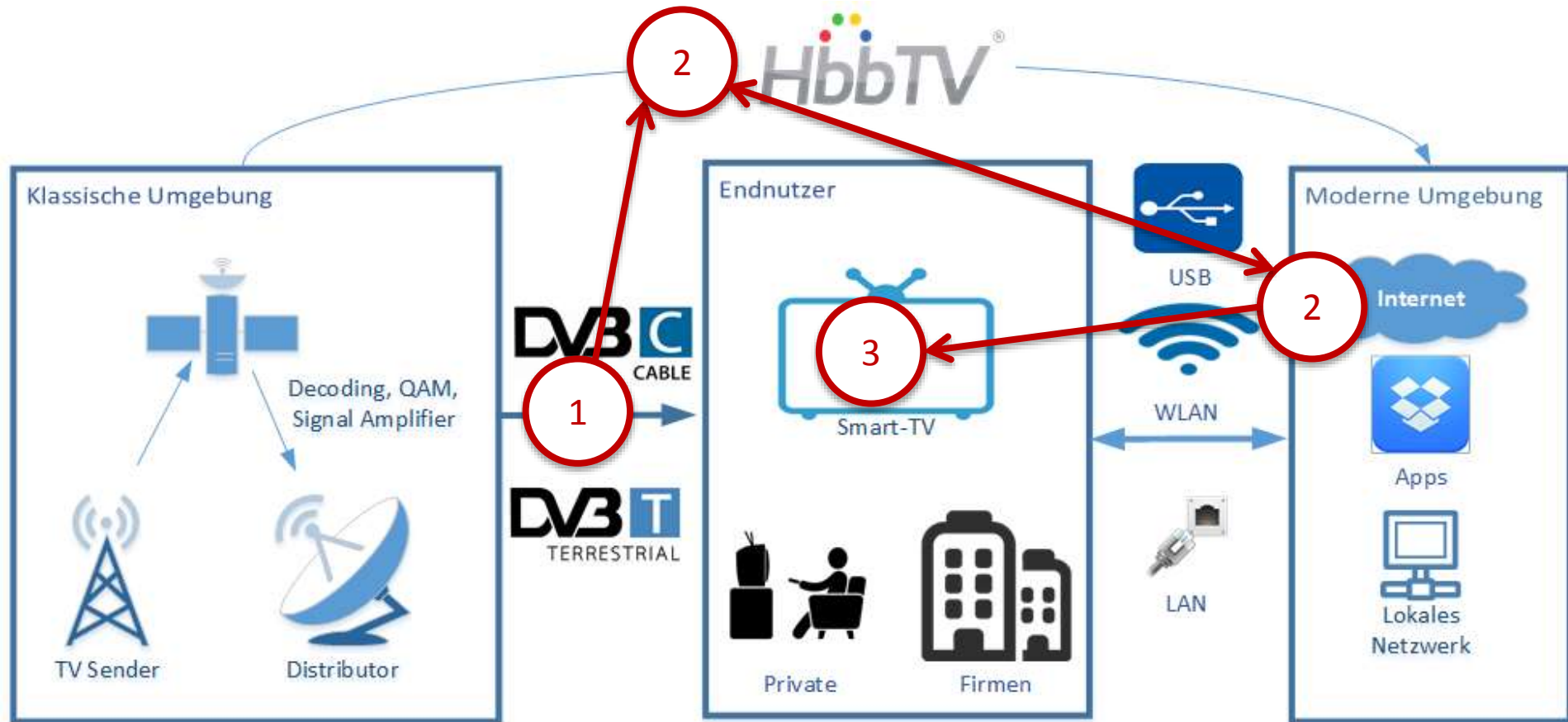


Unsere Ziele für einen Angriff

- ▶ Keine Benutzer-Interaktion notwendig
- ▶ Kein physischer Zugriff notwendig
- ▶ Möglichkeit für Angriffe auf breite Masse als auch spezifische Ziele
- ▶ Aktuelle Hard- und Software verwenden (z.B. Samsung OS)



Moderne TV-Umgebung





Demo Schritt 1: DVB angreifen

- ▶ DVB
 - ▷ Einwegkommunikation
 - ▷ Keine Absenderüberprüfung
- ▶ Möglichkeiten zur DVB-Signalübernahme
 - ▷ Angreifen der TV-Sender
 - ▷ DVB-T stärker senden
 - ▷ DVB-C Kabel unterbrechen



Demo Schritt 2: Seite aufrufen

- ▶ DVB-Ergänzung
 - ▷ In unserer Demo
- ▶ Nicht notwendig
 - ▷ DVB-Decoder ebenfalls anfällig
 - ▷ Noch nicht exploited

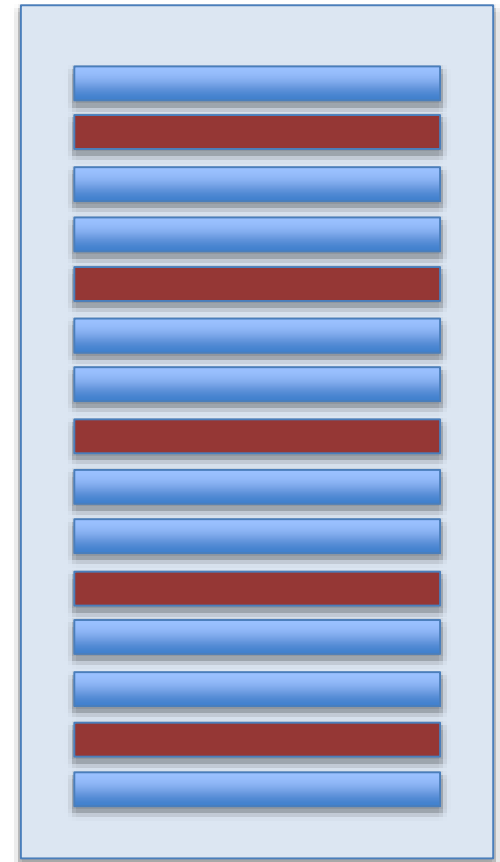


Demo Schritt 3: Flash Exploit

- ▶ Flash
 - ▷ Spannend und viel diskutiert
 - ▷ Gemeinsamer Nenner von vielen heterogenen Systemen
 - › Hacking Team
- ▶ Smashing the Heap with Vector
 - ▷ Weitverbreitete Flash Exploit-Methode
- ▶ Buffer Overflow: CVE-2015-3090
- ▶ Exploit einfach, Umfeld schwierig

Demo Schritt 3: Flash Exploit

- ▶ Simpler Prozess
- ▶ Grosser Vector
 - ▷ `new Vector.<Object>(1024)`
- ▶ Füllen mit kleinen Vektoren
 - ▷ `new Vector.<uint>(0xa6)`
- ▶ Löschen von einigen, nicht aufeinanderfolgenden kleinen Vektoren
- ▶ ShaderJob erstellen (wie bei Use-After-Free)
- ▶ ShaderJob Overflow triggern
 - ▷ Überschreibt Länge des kleinen Vectors



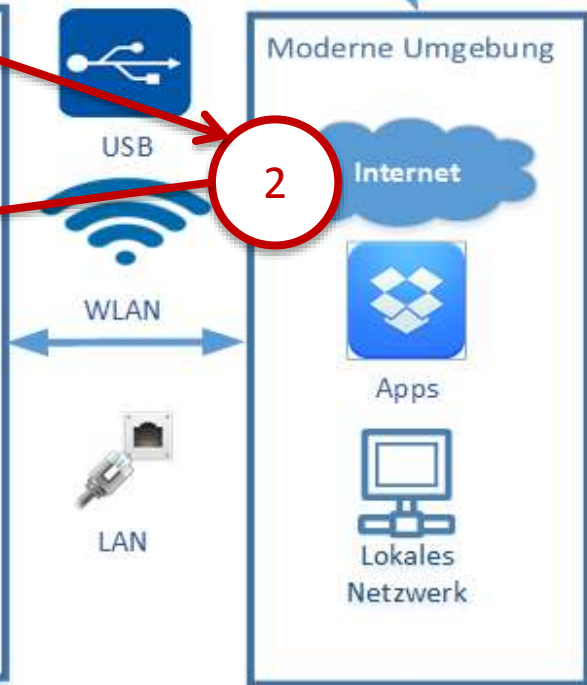
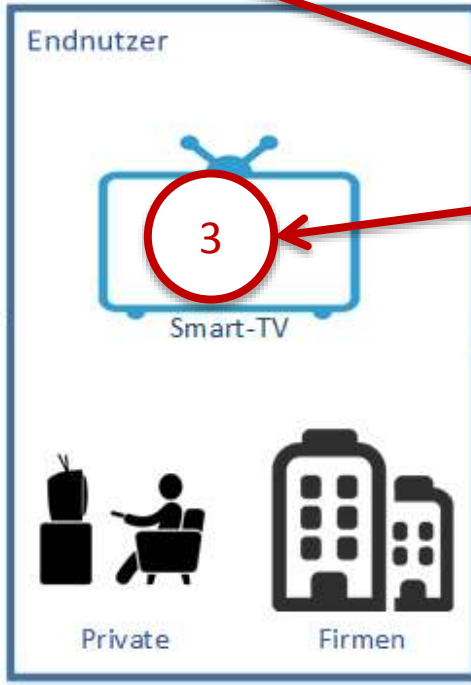
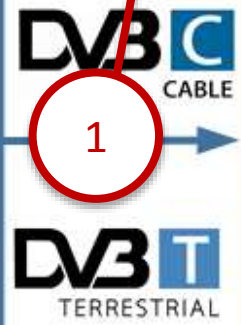
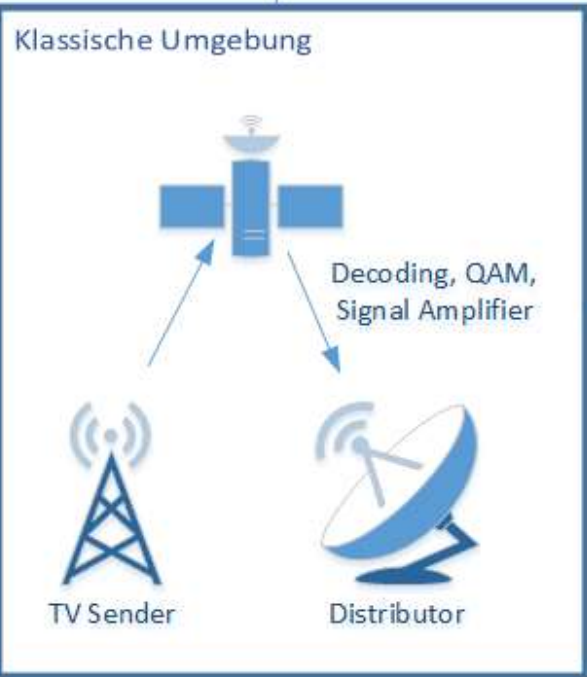


Demo Schritt 4: Post Exploitation

- ▶ Ausgereifte Post Exploitation Toolkits verfügbar
 - ▷ SamyGO
- ▶ Root Zugang
- ▶ Autostart
- ▶ Persistent, auch bei Firmware-Updates
- ▶ Reverse-Shell



Fazit





Fazit

- ▶ Angriff auf Signalquellen
 - ▷ Private Sender, Staat, Verteiler
- ▶ Gezielte Angriffe mit begrenzten Mitteln möglich
- ▶ Spurenloses Angreifen möglich

- ▶ «Web-Exploits» noch auf andere Architektur ausgerichtet
- ▶ Sicherheitsbewusstsein erwacht bei Smart-TV Herstellern