

SMART-TV

Glotze glotzt zurück

Hacker können internetfähige Fernseher mit einfachen Tricks in Videowanzen verwandeln – und so unbemerkt in fremden Wohnzimmern filmen.

Big Brother überwacht seine Untertanen, indem sein Gesicht auf Fernsehbildschirmen erscheint, von denen aus er in jede Wohnung spähen kann. So malt eine Verfilmung von George Orwells Roman „1984“ die Zukunft aus.

Die Realität erscheint fast noch gruseliger: Viele internetfähige Fernseher eignen sich zum Spitzeln – nur dass die Opfer nichts davon merken.

„Ich mache jetzt aus diesem Fernseher eine Videowanze“, sagt Benjamin Michéle, Sicherheitsforscher an der TU Berlin. Er schiebt einen USB-Stick in das handelsübliche Smart-TV. Auf dem Stick befindet sich ein harmlos wirkender Film, der sich mit dem Gerät abspielen lässt. Im Hintergrund programmiert derweil ein hundsgemeiner Schadcode den Fernseher um – und schon lässt dieser sich komplett übers Internet fernsteuern.

„So, das war's“, sagt Michéle nach ein paar Sekunden. Er sitzt vor seinem Notebook und greift nun auf das TV-Gerät zu. Der Nutzer sieht davon nichts, das Programm läuft weiter wie gehabt. Ein Tastendruck, schon sind Kamera und Mikro-

fon angeknipst. Michéle sieht und hört über seinen Rechner die Kollegen, die in Sichtweite des Fernsehers arbeiten, hier oben bei der Forschungsgruppe „Security in Telecommunications“ im 16. Stock des TU-Hochhausturms.

„Diese Sicherheitslücke ist weit verbreitet“, sagt Michéle: Die Filmwiedergabe, der sogenannte Mediaplayer, ist nicht ausreichend abgesichert. Michéle hat gerade seine Arbeit auf einer renommierten wissenschaftlichen Konferenz vorgestellt. Zufällig geht es bei ihm um Geräte von Samsung. Das bedeute jedoch nicht, dass sie anfälliger seien als andere, erklärt der Informatiker, Samsung sei einfach Marktführer.

In ihrer Empfindlichkeit gegenüber Hackerattacken wird deutlich, wie dumm die angeblich schlaunen Fernseher sich eigentlich gebärden. Wobei das Wort Fernseher hier in die Irre führt: Smart-TVs gleichen eher verkappten Linux-Rechnern mit besonders großem Bildschirm. Sie haben eine Menge Rechenpower – aber Virenschutz, Firewall, Rechtemanagement, kurzfristige Updates, wie herkömmliche Computer sie mitbringen? Fehlanzeige.

„Smart-TVs dürften bald ein beliebtes Ziel für Hacker werden“, sagt Michéle, denn so leicht, wie sie zu kapern sind, so vielseitig lassen sie sich missbrauchen: Paparazzi könnten Promis filmen, Einbrecher verlassene Wohnungen ausspionieren, Hacker Online-Angriffe koordinieren oder Pirateriebörsen betreiben. Eine Sicherheitsfirma hat bereits ein sogenanntes Botnet aufgespürt, eine Armee fremdgesteuerter Rechner, die teils aus vernetzten Kühlschränken und Smart-TVs bestand.

In rund zehn Millionen deutschen

Haushalten stehen bereits Internetfernseher, das ist ungefähr jeder vierte. In zwei Jahren könnten es doppelt so viele sein.

Wie kann es sein, dass eine milliarden-schwere Hightech-Industrie die einfachsten Sicherheitsvorkehrungen vergisst? Michéle war zunächst skeptisch, als er die Sicherheitslücke fand. Er kontaktierte vor mehr als zwei Monaten den Hersteller.

„Die beschriebenen Probleme sind uns bekannt“, antwortet der Hersteller auf Nachfrage des SPIEGEL. Und versichert, „dass alle nach dem Jahr 2011 produzierten Samsung Smart-TVs nicht betroffen sind“. Michéle dagegen sagt, die Schutzlücke betreffe auch Modelle von 2013.

Er ist in bester Gesellschaft, Forscher finden immer neue Sicherheitslücken bei Smart-TVs diverser Hersteller: Der koreanische Informatiker Kim Seungjoo etwa konnte Fernseher übers Netz fernsteuern. Derzeit testet er, ob er ein TV aus der Ferne auch zum Überhitzen bringen kann. Und die amerikanische Sicherheitsfirma Codenomicon brachte mit ein paar einfachen Tricks Fernsehgeräte zum Abstürzen.

Hinzu kommt das gewohnheitsmäßige Schnüffeln im Hintergrund: Die Computerzeitschrift „c't“ berichtete vor kurzem von Fernsehern, die Senderwechsel über die Funktion HbbTV notieren und an Spitzelservers übertragen zur Auswertung – sogar dann noch, wenn Nutzer diese Funktion abschalten.

Der südkoreanische Hersteller LG ging sogar noch weiter: Wenn Nutzer ihre eigenen Urlaubsfilme über einen USB-Stick auf dem Fernseher abspielten, schnüffelte dieser Dateinamen aus und übertrug sie an den Hersteller. Als das aufflog, stopfte man die Lücke mit einem Update.

Das Problem, das Michéle nun gefunden hat, übertrifft dabei alles Bekannte: „Neu ist, dass ich einen Fernseher übers Netz übernehmen kann, also ohne lokalen Zugang vor Ort. Und zwar über die ganz banale Medienwiedergabe.“

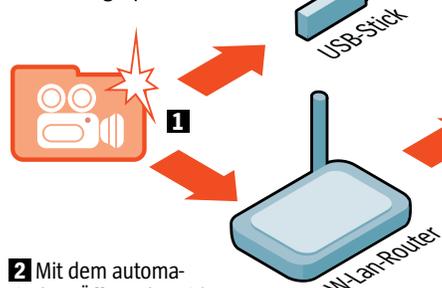
Michéle fordert, dass Hersteller dringend ihre TV-Software nachbessern. Er könnte sich auch eine unabhängige Prüfkommision vorstellen, die Sicherheitsgütesiegel für Fernseher vergibt. Andere Forscher wie Marco Ghigliari von der TU Darmstadt tüfteln an kleinen Firewall-Rechnern, um den tückischen Datenverkehr ihrer Glotzen zu drosseln.

Um sich zu schützen, setzen Sicherheitsprofis wie Michéle auf einen ungelungenen Notbehelf: Über die Kamera seines Fernsehers hat er ein Stück Papier geklebt. Und er schaltet ihn nicht mit der Fernbedienung aus, denn im Hintergrund könnte unbemerkt das Mikrofon weiterlauschen. Daher zieht er lieber den Stecker aus der Dose. Sicher ist sicher. HILMAR SCHMUNDT

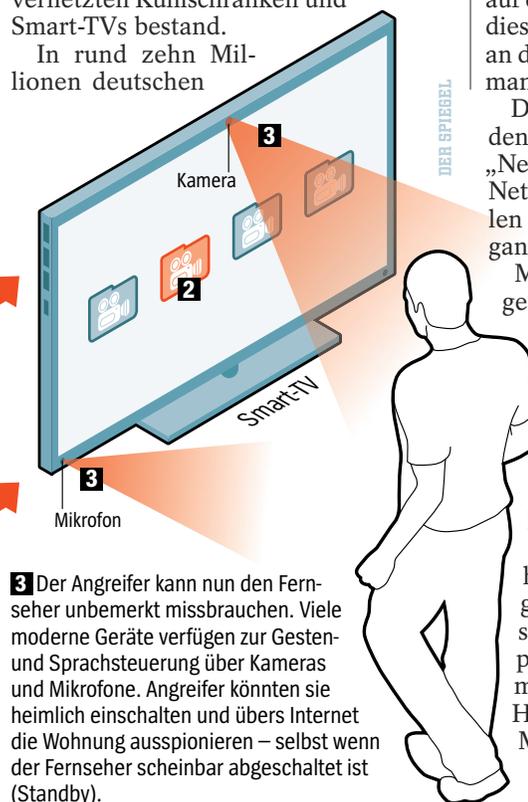
Manipulierte Mattscheibe

Wie internetfähige Smart-TVs ihre Nutzer ausspitzeln können

1 Eine manipulierte Videodatei wird zum Beispiel über einen USB-Stick oder über das Internet auf den Fernseher gespielt.



2 Mit dem automatischen Öffnen des Videos wird im Hintergrund ein Schadcode gestartet, der Angreifern die Fernsteuerung des Fernsehers ermöglicht. Der Besitzer bekommt davon nichts mit, der angeklickte Film wird scheinbar ganz normal abgespielt.



3 Der Angreifer kann nun den Fernseher unbemerkt missbrauchen. Viele moderne Geräte verfügen zur Gesten- und Sprachsteuerung über Kameras und Mikrofone. Angreifer könnten sie heimlich einschalten und übers Internet die Wohnung ausspionieren – selbst wenn der Fernseher scheinbar abgeschaltet ist (Standby).