IFA 2012: Smart TVs im Fokus von Cyber-Kriminellen

Warum die Homecomputer des 21. Jahrhunderts zu Zielscheiben werden könnten.

Smart TVs sind Fernseher mit einem integrierten Computer oder anders formuliert: Smart TVs werden oder sind zum Teil bereits die Heimcomputer des 21. Jahrhunderts. Anwender nutzen die internetfähigen TVs zum Surfen im Internet, installieren Apps oder setzen die modernen Geräte dank integrierter Video-Kamera und Skype für Video-Telefonie ein. Ebenfalls im Kommen sind kostenpflichtige Services, wie beispielsweise Online-Videotheken. Dort kann man sich die neuesten Spielfilme bequem per Klick als Stream ansehen. Um das alles zu realisieren, sind die Geräte mit leistungsstarken Prozessoren ausgestattet. Würde es Angreifern gelingen, die internetfähigen Geräte mit Schadcode zu infizieren, würde sich das für die Täter in mehrfacher Hinsicht lohnen: Von Datendiebstahl, über das Ausspähen des Wohnzimmers per Smart TV Kamera, bis hin zur Einbindung in Botnetze oder die Nutzung der geballten Rechenpower zum Knacken von Zugangsdaten, ist alles denkbar. Nach Einschätzung von G Data haben Smart TVs das Potential für einen neuen Schadcode-Hype.

Smart TVs erschließen kommerziellen Anbietern eine vollkommen neue Nutzergruppe: Menschen, die zuvor keinen Computer einsetzten oder nicht im Internet unterwegs waren, sind dank Smart TV jetzt online. Aber auch das bisherige Nutzerverhalten der Internet-Community könnte sich generell verändern: Wurde bisher ein Notebook oder ein Tablet-PC zum Surfen auf der Couch eingesetzt, könnten es zukünftig Smart TVs sein. Das Tablet oder das Smartphone wird hierbei lediglich zur Steuerung und als komfortable Tastatur eingesetzt. Ein enormes Kundenpotential für Shopping- Portale und für Anbieter kostenpflichtiger Dienste, wie beispielsweise Video-on- Demand Services. Ein Potential, das nach Einschätzung des G Data Sicherheitsexperten Ralf Benzmüller, unweigerlich auch Cyber-Kriminelle auf den Plan rufen wird.

Die Grenzen zwischen Smartphone, PC und Fernseher verwischen zunehmend. Auf Smartphones kann man fernsehen und mit dem Smart TV kann man surfen. Internet-Fernseher bieten potentielle Angriffsmöglichkeiten, die Malware-Autoren versuchen werden, auszunutzen, warnt G Data Sicherheitsexperte Ralf Benzmüller, Leiter der G Data SecurityLabs. Sollte es den Tätern gelingen, infizierte Apps in die Marktplätze der Hersteller einzuschleusen oder Smart TVs per Drive-by-Downloads zu infizieren, wären die Folgen nach Einschätzung des Experten nicht vorhersehbar. Es wäre nicht auszuschließen, dass heimische Fernseher in Zukunft für DDoS-Angriffe auf Unternehmen, Industrieanlagen oder zum Knacken von Passwörtern missbraucht werden. Nach unserer Einschätzung nutzen Cyber-Kriminelle bereits die frei zugänglichen Software-Entwicklungs-Kits der TV Hersteller, um Angriffsmöglichkeiten auszuloten. Wir rechnen damit, dass in Kürze die ersten Proof-of-Concepts veröffentlicht werden.

Warum sind Smart TVs für Angreifer interessant?
- Neue Zielgruppe: Dank Smart TVs erschließt sich den Tätern eine völlig neue Zielgruppe: Menschen, die bisher keinen Computer im Haushalt für das Internet nutzten, sind jetzt online. Die Zahl der internetfähigen Geräte multipliziert sich ebenso, wie die Online-Zeit der einzelnen Nutzer.

- Bezahldienste: Viele Smart TV-Nutzer könnten zukünftig den Fernseher statt den Computer zum Shoppen einsetzen und diesen auslassen. Wie bei PCs und Smartphones, sind persönliche Zugangsdaten der Besitzer, wie Login-Daten von kostenpflichtigen Angeboten oder von E-Mail-Konten, für Kriminelle bares Geld wert.

- Angriff per Smart-TV: Die Grafikprozessoren in den Fernsehern sind sehr leistungsfähig und eignen sich hervorragend zum Brute-Forcen von Passwörtern. Ein entsprechendes Botnetz von Fernsehern könnte die Dienstleistung Passwörter knacken sehr günstig und schnell erbringen.

- Private Daten im Visier: Viele Hersteller rüsten Geräte bereits mit einer integrierten Kamera und Skype aus. Hier besteht die Gefahr, ungewollt zum Medienstar zu werden, falls es den Tätern gelingt den Fernseher unter ihre Kontrolle zu bringen. Neben dem Verlust der Privatsphäre könnten Cyber-Kriminelle beispielsweise Informationen über die Wohnungsausstattung anderen Kriminellen anbieten die Folge: Einbrecher schauen einfach vorher nach, wie die Wohnung aussieht und ob sich ein Einbruch lohnt.

Womit müssen wir zukünftig rechnen?
Smart-TVs sind nur ein Beispiel einer zunehmenden Verwischung der bisherigen Geräte-Grenzen. Die Vernetzung unterschiedlichster Geräte und deren Anbindung ans Internet bietet eine Vielzahl von Chancen aber zugleich auch neue Angriffsvektoren für Cyber-Kriminelle. Die IT-Security-Industrie kann schnell auf die neuen Bedrohungen reagieren. Vielen Nutzern von Smart TVs muss allerdings noch bewusst werden, dass sie den gleichen Bedrohungen ausgesetzt sind, wie andere Rechner im Internet, prognostiziert Ralf Benzmüller, Leiter der G Data SecurityLabs. Es bleibt somit abzuwarten, wann der erste Schädling für Smart-TVs die Wohnzimmer erreichen wird.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/lhcsi8

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/ifa-2012-smart-tvs-im-fokus-von-cyber-kriminellen-95999

=== Smart TVs im Fokus von Cyber-Kriminellen (Bild) ===

Smart TVs sind Fernseher mit einem integrierten Computer oder anders formuliert: Smart TVs werden oder sind zum Teil bereits die Heimcomputer des 21. Jahrhunderts. Anwender nutzen die internetfähigen TVs zum Surfen im Internet, installieren Apps oder setzen die modernen Geräte dank integrierter Video-Kamera und Skype für Video-Telefonie ein. Ebenfalls im Kommen sind kostenpflichtige Services, wie beispielsweise Online-Videotheken. Dort kann man sich die neuesten Spielfilme bequem per Klick als Stream ansehen. Um das alles zu realisieren, sind die Geräte mit leistungsstarken Prozessoren ausgestattet. Würde es Angreifern gelingen, die internetfähigen Geräte mit Schadcode zu infizieren, würde sich das für die Täter in mehrfacher Hinsicht lohnen: Von Datendiebstahl, über das Ausspähen des Wohnzimmers per Smart TV Kamera, bis hin zur Einbindung in Botnetze oder die Nutzung der geballten Rechenpower zum Knacken von Zugangsdaten, ist alles denkbar. Nach Einschätzung von G Data haben Smart TVs das Potential für einen neuen Schadcode-Hype.

Shortlink:
http://shortpr.com/und9n1

Permanentlink:
http://www.themenportal.de/bilder/smart-tvs-im-fokus-von-cyber-kriminellen

=== Ralf Benzmüller, Leiter G Data SecurityLabs (Bild) ===

Ralf Benzmüller, Leiter der G Data SecurityLabs

Shortlink:
http://shortpr.com/b76ngm

Permanentlink:
http://www.themenportal.de/bilder/ralf-benzmueller-leiter-g-data-securitylabs-52864

=== G Data Software AG (Bild) ===

Shortlink:
http://shortpr.com/i49hbq

Permanentlink:
http://www.themenportal.de/bilder/g-data-ssoftware-ag

Pressekontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

presse@gdata.de

Firmenkontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

gdata.de
presse@gdata.de

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

Anlage: Bild