

BLACK HAT

## Gehackt: Geldautomat spuckt Scheine

29. Juli 2010, 12:19



### Was im Film "Terminator 2" bereits vor Jahren demonstriert wurde, funktioniert nun auch real

Mit den richtigen Hacker-Tricks bringt man Geldautomaten dazu, die enthaltenen Scheine auszuspuken. Was im Film "Terminator 2" bereits vor Jahren demonstriert wurde, funktioniert nun auch real. Das hat der Sicherheitsexperte Barnaby Jack, Mitarbeiter beim Security-Dienstleister IOActive, im Rahmen der Sicherheitskonferenz Black Hat vorgeführt.

"Das ist eine interessante Demonstration. Sie zeigt einmal mehr, dass kein System unangreifbar ist", meint Sicherheitsexperte Joe Pichlmayr, Geschäftsführer von

Ikarus Software. Ob derartige Geldautomaten-Hacks zum Massenphänomen werden, bleibt aber fraglich.

### Tiefgehende Schwächen

Jack hat bei der Demo Sicherheitslücken an zwei Geräten der Hersteller Tranax und Triton ausgenutzt. Der Forscher hatte die Geldautomaten vor einigen Jahren via Internet gekauft und ihre auf Windows CE basierende Software genau auf Fehler analysiert. So konnte er tiefgehende Schwachstellen aufspüren, die ihm eine umfassende Manipulation der Geräte erlaubt.

Im Rahmen seiner Vorführung hat Jack unter anderem mithilfe eines USB-Sticks einen Rootkit auf einem Geldautomaten installiert. Damit erlangt er die Kontrolle über das Gerät. So ist es dem Forscher möglich, auf dem Display das Wort "Jackpot" anzuzeigen, während der Automat Geldscheine ausspuckt. Dem Experten zufolge könnten Hacker manipulierte Geräte auch per Modemverbindung fernsteuern. Tranax und Triton haben die entsprechenden Sicherheitslücken mittlerweile geschlossen. Doch insgesamt hat Jack nach eigenen Angaben zufolge vier Geldautomaten-Modelle geknackt.

### Standortfrage

Bei den in der Demo angegriffenen Geräten handelt es sich um freistehende Geldausgabeautomaten, wie sie besonders in den USA oft in Hotels, Bars oder Geschäften zu finden sind. "Ein solch direkter Zugriff bietet einfach ganz andere Möglichkeiten, als wenn ein Angriff über ein gesichertes Netzwerks erfolgen müsste", betont Pichlmayr. Daher sind freistehende Geräte deutlich angreifbarer als fest verbaute Geldautomaten in Banken. Dort würde dank Videoüberwachung oder teils speziellen Sensoren eine physische Manipulation auffallen.

Zudem ist die Frage, wie leicht Cyberkriminelle an die nötigen Mittel für tiefgehende Attacken kommen. Immerhin hat Jack die Software der Automaten über Jahre analysiert, um seine Tools zu entwickeln. Diese wird er nach Angaben gegenüber Cnet definitiv nicht veröffentlichen. Wer also bei Geldausgabegeräten ebenfalls den Jackpot landen will, müsste wohl bei Null beginnen. (pte)

### Link

Black Hat