Cyber-Kriminalität

Computervirus befällt Geldautomaten dank Windows XP

Als sogenannte Schläfer kannte man bislang Agenten oder Terroristen. Aber es gibt auch Schadprogramme, die Schläfer sind: Nachdem sie auf Computer gelangt sind, nisten sie sich ein und werden für lange Zeit nicht aktiv. Ausgerechnet in einem Geldautomaten wurde nun ein Programm entdeckt, das auf Wunsch sogar Geld ausgibt - aber auch die geheimen Daten der Kunden sammelt.

von Michael Voß, MDR AKTUELL

Der virus "Skimmer" kann Kartennummer und PIN lesen.

Bildrechte: Colourbox.de

Entdeckt wurde das Programm von der IT-Sicherheitsfirma "Kaspersky Lab". Bei einer Routine-Untersuchung in einer russischen Bank bemerkte sie, dass Hacker in deren Netzwerk eingedrungen waren. PC-Virenforscher Sergey Golovanov war dabei: "Leider fanden wir zunächst keine weiteren Spuren. Kein Geld wurde abgehoben, nichts war gestohlen oder angefasst worden. Als wir dann anfingen, die Bankautomaten zu überprüfen, haben wir das Schadprogramm gefunden."

"Skimer" liest Daten und spuckt Geld aus

Das Programm heißt Skimer und ist schon seit 2009 bekannt. Doch es wurde weiterentwickelt: Wie ein Schläfer bleibt es ruhig, nachdem es in das jeweilige Netzwerk eingeschleust wurde. Wer es aufwecken will, muss am Geldautomaten eine manipulierte EC- oder Kreditkarte einführen: Der Magnetstreifen enthält zusätzliche Informationen, die das Programm starten. Sergey Golovanov erklärt: "Wenn die Täter die spezielle Karte einführen, können sie direkt Bargeld abheben, ohne irgendetwas einzugeben. Die Karte kommt von selbst wieder heraus und danach wird das Geld ausgegeben - dieses süße Geräusch! Und gleich kommen da 40 Scheine aus jeder Kassette heraus."

Ein anderer Befehl speichert beispielsweise Daten der Kunden, die vorher an dem Geldautomaten waren, auf dem Chip der eingeführten Karte. PIN und Kartennummern gelangen so in falsche Hände, ohne dass die Bank diesen Datenverlust überhaupt

Windows XP erhält schon längst keine Sicherheits-Updates mehr.

Bildrechte: IMAGO

bemerkt. Möglich ist das, weil weltweit viele Bankautomaten noch immer das 15 Jahre alte Betriebssystem Windows XP nutzen. Microsoft selbst rät von Windows XP ab - seit zwei Jahren werden keine Sicherheits-Updates mehr geliefert. Damals waren noch 95 Prozent aller Geldautomaten mit dem System ausgerüstet.

Versicherungen ersetzen Verlust

Für die deutsche Kreditwirtschaft und deren Kunden sei das alles unerheblich, sagt Kerstin Altendorf vom Bundesverband deutscher Banken: "Unabhängig von allen möglichen Bedrohungs-Szenarien ist der Bankkunde immer vor Schäden geschützt, für die er nicht selbst verantwortlich ist. Selbst wenn der unwahrscheinliche Schadensfall eintreffen sollte, bleibt er nicht auf seinem finanziellen Verlust sitzen." Klar, denn in diesem Fall zahlt die Versicherung. Weder dem Kunden noch der Bank entsteht ein Schaden. Deshalb ist für Experten klar: Für die Bank lohnt es sich nicht, das System schnell zu modernisieren - den Schaden haben ja die Versicherungen.

Doch die Banken wissen ganz offensichtlich, dass die Situation immer gefährlicher wird. Vor zwei Jahren hieß es in einer Pressemitteilung: "Ein weiterer wirksamer Schutz vor Angriffen ergibt sich aus der Tatsache, dass die Geldautomaten der Deutschen Kreditwirtschaft nicht über das offene Internet erreichbar sind." Dieser zusätzliche Schutz wird in der aktuellen Stellungnahme nicht mehr erwähnt. Nachfragen dazu waren nicht möglich.

Zuletzt aktualisiert: 27. Mai 2016, 10:21 Uhr

Die Kommentierungsdauer ist abgelaufen. Der Beitrag kann deshalb nicht mehr kommentiert werden.

5 Kommentare

28.05.2016, 12:56 5

| Krause - "ich bin ja ein Nazi, aber"

@ 4: 'Umstieg auf Unix/Linux' ist so pauschal revolutionär. Das bissl Bildschirmausgabe läßt sich auch mit Windows verschönern. Der Fehler sitzt zumeist nicht im Computer, sondern davor! ;) ... Weniger ist mehr: je weniger der 'Gegner' der IT-Sicherheit über das System erfährt, desto sicherer wird es. Aber

wenn der Arbeitsbildschirm der 'Bankomaten' auch nur der einzige ist, dann werden nun mal auch Systemnachrichten über ihn ausgegeben... und das, wo einem die 7"-Displays hinterher geschmissen werden... am faschen Ende gespart! ;)

28.05.2016, 10:42 | **J.R.** 4

@Krause:
Genau deshalb bitte Umstieg auf Unix/Linux. Diese Systeme sind so perfekt anpassbar dass man auch Fehlermeldungen entsprechend anpassen kann und nicht der Benutzer des "Bankomat" in Ruhe rauslesen kann was denn schief gegangen ist. Sowas ist absolut das Schlimmste! Aber ja, ich gebe Dir recht: Die Software ist immer nur so gut wie der Programmierer vor dem Bildschirm.

27.05.2016, 11:42 | **Krause - "ich bin ja ein Nazi, aber"** 3

Es liegt schwerlich nur an der OS-Version, ob ein Bargeldautomat selbst oder das ganze bankinterne Netzwerk kompromittiert werden kann: wer solche weitverbreiteten OS's, die für Privat- und normale kommerzielle Geschäftsanwender konzipiert sind, unverändert in sicherheitsrelevanten Systemen von Banken o.ä. einsetzt, der handelt schon grob fahrlässig. Ich selbst bin mit XP zufriedener denn je, seit MS nun die Finger davon läßt, obwohl ich es immer weniger nutze. Aber egal, ob Windows, Linux oder Unix: gerade eine Bank sollte im Umgang mit elektr. Kundendaten immer eigene Sicherheitsmaßnahmen treffen. Dieser Punkt sollte in die Bewertung der Schadensversicherung mit einfließen, um Banken dafür mehr zu motivieren. Der 'Bankomat' meiner Hausbank hatte sich letztens aufgehangen und stand nun mit einer Fehlermeldung eines identifizierbaren OS herum: allein das ist schon ein No-Go! IT-Sicherheit ist nun mal nichts für Amateure! Rechner von heute bieten genug Potential - man muß es nur nutzen.

27.05.2016, 08:40 | **J.R.** 2

Ich hoffe die Banken wachen endlich mal auf diese Windows-Systeme abzuschaffen und auf sicherere Wege mit Linux/Unix/BSD zu setzen. Hier ist es (fast) egal wie alt ein System ist. Sicherheitsupdates werden immernoch geliefert und man wird nicht von einem Großkonzern "gezwungen" auf Grund der eigenen IT-Sicherheit denen Geld zu bezahlen nur für neue Software.

27.05.2016, 08:27 | **Olli D.** 1

Und in den Atomkraftwerken läuft Windows NT.