Warum Bankräuber keine Pistole mehr brauchen

Warum Bankräuber keine Pistole mehr brauchen

Geldautomaten in sicherer IT-Umgebung vor Angriffen abschirmen
"Hände hoch, das ist ein Überfall!" - diesen Satz hören Bankangestellte heutzutage bei weitem nicht mehr so häufig wie früher. Denn moderne Bankraubmethoden finden gar nicht mehr vor Ort statt, sie sind viel raffinierter geworden. Mittlerweile attackieren Kriminelle direkt auf der Software-Ebene, um Kontrolle über die Geldautomaten zu erlangen und sie anschließend auszuräumen. Aber auch Online-Banking-Nutzer sind gefährdet, da z.B. über Phishing-Mails die Eingabe ihrer Login-Daten forciert wird, die die Verbrecher dann abgreifen und das Konto plündern. Damit es gar nicht erst soweit kommt, errichtet die SecureBox-Software des IT-Security-Entwicklers COMODO eine abgeschirmte IT-Betriebsumgebung, die beliebige Applikationen "containerisiert" ausführt.
Prinzipiell ist ein Geldautomat ein Endpoint-Gerät im Netzwerk einer Bank. Die meisten Geräte laufen auf einem Windows-Betriebssystem und sind daher ebenso wie Computer angreifbar. Nicht wenige Automaten basieren noch auf dem Betriebssystem Windows XP, für das Microsoft den Support im April 2014 eingestellt hat - und damit diese Geräte zu einem attraktiven Ziel von Hackern gemacht hat.
Sicherer Hort in gefährlicher Umgebung
Auf dieser Sichtweise basiert die Herangehensweise von COMODO: Es wird davon ausgegangen, dass die Endgeräte bereits mit Malware infiziert sind. Verglichen mit anderen Herstellern, die annehmen, dass die sichere Umgebung Angriffen von außen ausgesetzt ist, bildet COMODO eine Trutzburg innerhalb einer bösartigen, kompromittierten Umgebung. In dieser "sicheren Burg", einem speziell abgeschirmten Container, werden alle vertrauenswürdigen Anwendungen ausgeführt. Diese Containment-Technologie verhindert, dass unbekannte und gefährliche Applikationen eindringen und ihren Schadcode streuen können. Auch kann sie von keinem anderen Programm, das auf dem Endgerät oder im Netzwerk installiert ist, manipuliert werden.
Geldautomaten und Online-Banking abkapseln
Installiert eine Bank SecureBox im Betriebssystem ihrer Geldautomaten, blockiert sie damit Kompromittierungen und Hacking-Angriffe direkt am Ansatz. Denn da die Software der Automaten nur noch innerhalb der SecureBox ausgeführt wird, sind Angriffe von außen nicht mehr möglich. Ebenso lassen sich Online-Banking-Vorgänge sowie die Kommunikation von Mitarbeitern untereinander sowie mit Kunden sicherheitstechnisch härten. Dazu kann das Finanzinstitut seine Online-Banking-Software auf seiner Website in entsprechende Container einbinden. Dadurch startet der Kunde bei Anmeldung die Managementkonsole direkt in einem abgekapselten Container und ist damit immun gegen kriminelle Attacken; selbst dann, wenn sein eigener Rechner bereits infiziert sein sollte. Vorhandene Malware wird vom Container abgeblockt, da sie als unbekannte Applikation Zugriff verlangt. Diese Vorgehensweise ist ebenso mit einem kompletten Browser möglich, sodass Kunden ausschließlich den von ihrer Bank bereitgestellten, abgekapselten Browser nutzen können. Mittels SecureBox wird so z.B. das Abgreifen von Nutzerdaten über Keylogging-Methoden unterbunden.
Breit gefächertes Anti-Malware-Repertoire
Neben Anti-Keylogging-Maßnahmen bietet SecureBox weitere Schutzmechanismen, darunter aktive Virusentfernung, Remote Takeover Protection (proaktive Virenerkennung) und Anti-SSL Sniffing. Dabei prüft die Software Zertifikate auf Echtheit und verhindert im Manipulationsfall Man-in-the-middle-Angriffe. Ebenso ist das Auslesen des Speichers (Memory Scraping) unmöglich, da SecureBox keinerlei Zugriffe von externen Programmen zulässt.
Weitere Informationen sind auf der COMODO-Website zu finden.
Über COMODO:
COMODO wurde im Jahr 1998 gegründet und hat sich zunächst einen Namen als Anbieter von SSL-Technologien gemacht. Mit seinen SSL-Lösungen verfügt COMODO mittlerweile über einen weltweiten Marktanteil von etwa 27 Prozent. Heute entwickelt COMODO zudem Anti-Virus-Lösungen für Endanwender und den professionellen Einsatz. Durch das zum Patent angemeldete Auto-Sandbox-Verfahren lässt sich nachweislich ein fast einhundertprozentiger Schutz vor Malware garantieren. Die COMODO-Unternehmen beschäftigen mehr als 800 Mitarbeiter mit Hauptsitz in New Jersey/USA und weltweiten Niederlassungen in Großbritannien, der Türkei, Rumänien, China, der Ukraine, den Philippinen und Indien. Mehr als 55 Prozent der COMODO-Mitarbeiter an den verschiedenen Standorten sind in der Forschung und Entwicklung tätig. Verteilt auf die unterschiedlichen Zeitzonen betreibt COMODO fünf Virenlabore. Diese Virenlabore gewährleisten rund um die Uhr die zuverlässige Erkennung und Bekämpfung von Schädlingen aus dem Internet. Weitere Informationen unter: www.COMODO.com .

Ansprechpartner COMODO Deutschland
Karl Hoffmeyer
Bleichstraße 3
D-33102 Paderborn
Tel.: +49(0)172 / 4351289
E-Mail: karl.hoffmeyer@COMODO.com
Web: www.COMODO.com
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
Marius Schenkelberg
Tel.: +49(0)2661 / 912600
E-Mail: ms@sprengel-pr.com
Web: www.sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=580739" width="1" height="1">

Pressekontakt

Comodo

33102 Paderborn

karl.hoffmeyer@COMODO.com

Firmenkontakt

Comodo

33102 Paderborn

karl.hoffmeyer@COMODO.com

Über Comodo:Comodo wurde im Jahr 1998 gegründet und hat sich zunächst einen Namen als Anbieter von SSL-Technologien gemacht. Mit seinen SSL-Lösungen verfügt Comodo mittlerweile über einen weltweiten Marktanteil von etwa 27 Prozent. Heute entwickelt Comodo zudem Anti-Virus-Lösungen für Endanwender und den professionellen Einsatz. Durch das zum Patent angemeldete Auto-Sandbox-Verfahren lässt sich nachweislich ein fast einhundertprozentiger Schutz vor Malware garantieren. Die Comodo-Unternehmen beschäftigen mehr als 800 Mitarbeiter mit Hauptsitz in New Jersey/USA und weltweiten Niederlassungen in Großbritannien, der Türkei, Rumänien, China, der Ukraine, den Philippinen und Indien. Mehr als 55 Prozent der Comodo-Mitarbeiter an den verschiedenen Standorten sind in der Forschung und Entwicklung tätig. Verteilt auf die unterschiedlichen Zeitzonen betreibt Comodo fünf Virenlabore. Diese Virenlabore gewährleisten rund um die Uhr die zuverlässige Erkennung und Bekämpfung von Schädlingen aus dem Internet. Weitere Informationen unter: www.comodo.com.