kaspersky BRING ON THE FUTURE

Leitfaden für sichere Geldautomaten und POS

Kaspersky Embedded System Security

Embedded Systems befinden sich überall um uns herum: in Geräten wie Ticketautomaten und Terminals über medizinische Geräte bis hin zu Geldautomaten und PoS-Systemen. Diese Geräte und die darauf ausgeführten Systeme weisen äußerst spezifische Sicherheitsanforderungen auf: Sie sind geografisch verteilt, nur schwer zu verwalten und nutzen oftmals veraltete Software. Und in den meisten Fällen reicht der bestehende Schutz (sofern überhaupt vorhanden) nicht aus, um sich vor immer umfangreicheren modernen Bedrohungen für Embedded Systems zu schützen. Unternehmen benötigen hierfür mehrstufigen und intelligenten Schutz, der speziell für diese Systeme entwickelt wurde.

Die Bedrohungslage

Geldautomaten und PoS-Systeme sind beliebte Ziele für Cyberkriminelle. Geldautomaten werden bereits seit 2008 angegriffen. Mit „Backdoor.Win32.Skimer" wurde damals das erste schädliche Programm entdeckt, das auf Geldautomaten abzielte. 2017 trat dann der erste Fall von Malware-as-a-Service speziell für Geldautomaten auf: Cyberkriminelle fügten alle nötigen Schadprogramme mit Videoanweisungen in einem Paket zusammen und boten dieses Paket jedem Interessenten an, der selbst Geldautomaten hacken wollte. Im selben Jahr entdeckten Kaspersky-Forscher bis dato unerkannte Angriffe auf Geldautomaten, bei denen neue Malware sowie Remote- und dateilose Vorgänge zum Einsatz kamen.

In den ersten neun Monaten 2019 war die Anzahl der Malware-Infektionen bei Geldautomaten/PoS-Systemen bereits höher als im gesamten Jahr 2018. Experten gehen davon aus, dass Angriffe über Software, die speziell auf Finanzunternehmen zugeschnitten ist, darunter auch Software für Geldautomaten und PoS-Terminals, weiterhin zunehmen werden. PoS-Attacken zählen zu den drei beliebtesten Angriffsmustern.

Cyberkriminelle greifen Embedded Systems an, um Bargeld, Kreditkarteninformationen und personenbezogene Daten zu stehlen oder in Systeme einzudringen. Hierbei sind Malware-basierte Angriffe oder Änderungen an Betriebssystem, Bibliothek oder Middleware beliebte Methoden, um erst die Kontrolle über angegriffene Geräte zu erlangen und dann über jedes Gerät im angeschlossenen Netzwerk. Jüngste Angriffe auf PoS-Anbieter führten im Verlauf auch zu Folgeattacken auf ihre Kunden.

Dieses Szenario wird durch einige spezifische Probleme von Geldautomaten und PoS-Systemen weiter verschärft.

Spezifisch Herausforderungen

Veraltete Software

Die Mehrheit der Banken wartet mit der Aufrüstung ihrer Geldautomaten, bis sie das Ende ihres Lebenszyklus erreicht haben. So sind die Systeme oft bis zu zehn Jahre im Einsatz, bevor sie ausgetauscht werden. Darüber hinaus werden meist gleich die gesamten Geräte ersetzt (vollständig mit neuer Software), anstatt die Software vorhandener Geräte zu aktualisieren, wenn neue Versionen veröffentlicht werden. Neben neuesten Bedrohungen für Embedded Systems bleibt auch alte Malware für Geldautomaten und PoS-Systeme – von denen sich einige bereits seit 2009 im Umlauf befinden – bis heute aktiv.

Windows XP ist nach wie vor eines der beliebtesten Betriebssysteme für Geldautomaten und PoS-Geräte. Trotz der Einstellung des offiziellen Supports 2014 nutzen die meisten Geldautomaten bis heute Windows XP Professional for Embedded Systems.

Angriffsschema bei Geldautomaten
Geografisch verteilte Geldautomaten eignen sich ideal für die Infektion mit Malware im Rahmen eines zielgerichteten Angriffs. Grund hierfür sind USB-Anschlüsse und Tastaturen, die leicht zugänglich im Wartungsfach an der Rückseite der Geldautomaten untergebracht sind, das lediglich durch ein einfaches Schloss gesichert ist.

Doch in vielen Fällen müssen Angreifer dieses Schloss gar nicht erst knacken. Denn es ist nicht unüblich, dass Wartungsmitarbeiter vor Ort ein semi-permanentes USB- oder LAN-/Modemkabel anbringen, das aus dem Wartungsfach des Geldautomaten herausführt, um sich das ständige Auf- und Zuschließen des Fachs zu ersparen.

Eine Verbesserung der Sicherheit durch eine einfache Deaktivierung der USB-Anschlüsse oder CD-/DVD-Laufwerke im Fach ist faktisch nicht machbar, da Wartungsmitarbeiter diese regelmäßig für die Instandhaltung des Automaten verwenden müssen.

Sobald eine Malware auf einem Geldautomaten installiert wurde, kann sie dort für einige Zeit versteckt existieren, wobei das System weiterhin wie gewohnt funktioniert, während die Software Daten sammelt und Vorbereitungen für den eigentlichen Angriff trifft.

Wenn der richtige Zeitpunkt gekommen ist, kann eine bestimmte Karte oder PIN eine Änderung in der Systemsteuerung auslösen, was dazu führt, dass jeder infizierte Geldautomat seine Inhalte auf Anforderung an die Cyberkriminellen weitergibt.

Sicherheitsanforderungen von Geldautomaten

- Die meisten Geldautomaten laufen mit Windows XP, das nicht mehr direkt von Microsoft unterstützt wird.
- Bedienfeld leicht zu erreichen
- Aktivierte USB-Ports und CD-/DVD-Laufwerke
- Konnektivität ist für die Bearbeitung finanzieller Transaktionen unerlässlich
- Middleware muss rechtlich gesehen ohne bestätigte Transaktionen mit der Geldautomaten-Hardware funktionieren.

PoS-Sicherheitsanforderungen

- Ransomware
- Keylogger
- Memory Dumper
- Network Sniffer (können auf dem PoS installiert werden, ist jedoch selten)
- Erfassung verifizierter persönlicher Daten
- Beliebter Einstiegspunkt für Advanced Persistent Threats (APT)

Schutz vor neuesten Bedrohungen

Kaspersky Embedded Systems Security bietet mehrere grundlegende Sicherheitsebenen, wie z. B. Systemkontrolle, Malware- und Netzwerkschutz, um Geldautomaten und PoS-Systeme vor neuesten Bedrohungen zu schützen.

Entwickelt für Embedded Systems

Kaspersky Embedded Systems Security bietet auch für Low-End-Systeme, die in nahezu allen Geldautomaten und PoS-Systemen zum Einsatz kommen, umfassende Sicherheit. Die Anforderungen beginnen bei nur 256 MB RAM.

Windows XP oder höher

Am 12. Januar 2016 beendete Microsoft den Support für Windows XP Embedded und am 12. April 2016 auch den für Windows Embedded for Point of Service. Kaspersky Embedded Systems Security bietet weiterhin 100-prozentige Unterstützung für das gesamte Windows-Portfolio: von Windows XP bis hin zum neuesten Windows 10.

Konformität mit PCI DSS

Die Funktionen von Kaspersky Security for Embedded Systems entsprechen den folgenden Unterpunkten von PCI DSS 3.2: 1.4, 2.4a, 5.1, 5.1.1, 5.2, 5.3, 6.2, 10.5.5, 11.5.

Komfort über Sicherheit?

Ein klassischer Schwachpunkt bei PoS-Systemen ist die Middleware, auf der sie basieren. Diese Middleware wird meist von Drittanbietern oder internen Abteilungen entwickelt. Bei der Entwicklung spielt Funktionalität oft eine wichtigere Rolle als Sicherheit und – wie auch bei Geldautomaten – sehen Anbieter im einfachen Zugang zu USB-Anschlüssen und CD-/DVD-Laufwerken eher einen Vorteil als eine Schwachstelle.

Die meisten PoS-Systeme verarbeiten Kredit-/Debitkarten und unterliegen daher, wie auch Geldautomaten, den PCI-DSS-Richtlinien. Alle Systeme verarbeiten ohne Ausnahme personenbezogene Kundendaten. Für den Schutz dieser Daten ist der Eigentümer des PoS-Systems verantwortlich. Ferner sind alle PoS-Geräte mit einem Intranet verbunden, wodurch sie zu einem praktischen Einstiegspunkt für zielgerichtete Angriffe werden.

Standort und Geräte

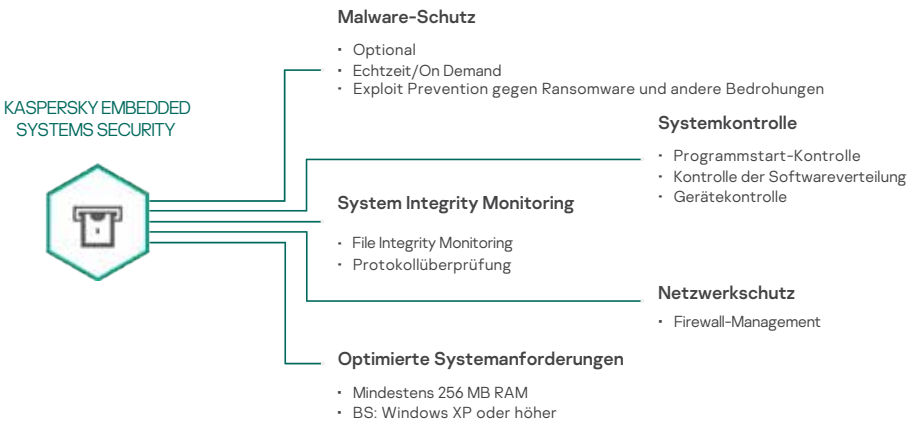
Weitere Probleme bei Geldautomaten und PoS-Systemen sind der physische Standort der Geräte sowie ihre Verwendung: Sie befinden sich stets an öffentlichen Orten und jedes System wird von Tausenden verschiedenen Nutzern verwendet. Darüber hinaus werden sie in der Regel von Drittanbietern gewartet.

In dieser Umgebung mit ihren spezifischen Herausforderungen ist ein Ansatz mit nur einer Technologie (also nur Virenschutz oder nur Default Deny) nicht wirksam und bieten keinen ausreichenden Schutz. Und durch die Einschränkungen von Geldautomaten und PoS-Systemen (schwache Kanäle, Low-End-Hardware und veraltete Software) gestaltet sich die Installation von Antivirensoftware oft kompliziert und unpraktisch. Entsprechend können Bedrohungen für Geldautomaten und PoS-Systeme weiterhin tagtäglich in die Geräte von Finanzdienstleistern und Einzelhändlern auf der ganzen Welt eindringen.

Nur mehrstufiger Schutz, der speziell für diese spezifischen Herausforderungen entwickelt wurde, kann entsprechende Systeme zuverlässig und erfolgreich schützen.

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security wurde speziell für Unternehmen mit Geldautomaten und PoS-Systemen entwickelt, um in diesem speziellen Bereich die Sicherheit zu gewährleisten. Die Lösung schützt die individuellen Schwachstellen entsprechender Architekturen, berücksichtigt hierbei die einzigartigen Funktionen sowie die Betriebssystem-, Kanal- und Hardwareanforderungen und unterstützt auch weiterhin Windows XP. Eine einzige intuitive Konsole bietet die Kontrolle und Transparenz, die Sie benötigen, um die effiziente, mehrstufige Sicherheit für Ihre Endpoints, kritischen Systeme und die gesamte IT-Infrastruktur zentral zu verwalten.



Kaspersky Embedded Systems Security schützt effizient auch schwierige Systeme wie Geldautomaten und PoS-Geräte, erfüllt vollständig die relevanten PCI-DSS-Anforderungen und ermöglicht es Anbietern, veraltete Hard- und Software schrittweise zu ersetzen.

Kontaktieren Sie das Kaspersky Enterprise Sales Team, um mehr über die effektive Sicherung Ihrer kritischen Bezahlsysteme zu erfahren.

Cyber Threats News: https://de.securelist.com
Neuigkeiten zur IT-Sicherheit: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency.

Getestet.
Transparent.
Unabhängig.