Kaspersky® Embedded Systems Security

Leitfaden für sichere Geldautomaten und POS

Standardmäßige Sicherheitsvorschriften für Embedded Systems neigen dazu, nur virenschutzbasierte Sicherheit oder Systemhärtung abzudecken, was nicht genug ist. Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von Embedded Systems nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde. Es ist an der Zeit, bewährte Technologien wie Gerätekontrolle und Default Deny wo erforderlich mit einem zusätzlichen Virenschutzmodul für kritische Systeme anzuwenden.

Embedded Systems bringen besondere Sicherheitsrisiken mit sich. Diese Systeme sind geographisch oft weit verteilt und daher schwer zu verwalten. Außerdem werden Sie nur selten aktualisiert. Geldautomaten und POS-Systeme sind ein beliebtes Ziel für Cyberkriminelle, da sie echtes Geld und Kreditkartendaten verarbeiten. Deshalb benötigen diese Systeme eine höchst fokussierte und intelligente Sicherheitslösung.

Risiken

Veraltete Software ist ein sehr häufig anzutreffendes Problem, und nicht nur Betriebssysteme von Kunden sind betroffen. Es ist bekannt, dass sich immer noch einige Satellitensysteme mit Jahrzehnte alter Hard- und Software in Betrieb befinden. Auch industrielle Kontrollsysteme stehen vor dem Problem, dass Betriebssysteme sehr alt und Erneuerungszyklen langwierig sind. Dasselbe gilt auch für Banksysteme: Häufig werden nicht nur Endpoints sondern auch interne automatisierte Banksysteme viele Jahre lang nicht aktualisiert. Bei Geldautomaten warten 80 % der kleineren Banken oftmals bis zum nächsten Ende eines Zyklus (was 5 bis 10 Jahre oder länger dauern kann), bevor sie neue Automaten kaufen, auf denen die aktuelle Software bereits installiert ist, anstatt die Software auf den vorhandenen Geldautomaten zu aktualisieren.

Windows XP ist nach wie vor eines der beliebtesten Betriebssysteme für Geldautomaten und POS-Systeme. Das Ende der Supportleistungen für dieses Betriebssystem wirkte sich auf eine Vielzahl an Unternehmen und Regierungsstellen aus. Banken und Einzelhandel betreiben weltweit viele Geldautomaten mit Windows XP Professional für Embedded Systems, daher waren diese Sektoren ganz besonders betroffen. Der Support für dieses System wurde schon im April 2014 gemeinsam mit der Kundenversion von Windows XP eingestellt.

Der Wechsel der Software von Geldautomaten und POS-Systemen ist im Allgemeinen ein langwieriger, kostspieliger und komplexer Prozess. Abgesehen vom Wechsel der Software bedeutet dies oft auch den Austausch einer nach wie vor funktionsfähigen, wenn auch technisch veralteten, Hardware.

Die Bedrohungslage

Geldautomaten, die außerhalb der physischen Sicherheitsumgebung der Bank betrieben werden und echtes Geld enthalten, sowie POS-Systeme, die verifizierte personenbezogene Daten und Kreditkarteninformationen verarbeiten, stehen daher zwangsläufig ganz oben auf der Hitliste von Cyberkriminellen.

Seit dem Jahr 2009, als es im Rahmen der Aktivitäten der Skimer-Malware den ersten ernstzunehmenden Angriff auf Geldautomaten gab, ist die Anzahl und Qualität der Angriffe in den darauffolgenden Jahren drastisch gestiegen. 2015 erreichten die Angriffe auf Geldautomaten und POS-Systeme einen neuen Höhepunkt. Dabei kam unter anderem folgende Malware zum Einsatz: Ploutus, Tyupkin, Carbanak, CardStealer, vSkimmer, Chewbacca, POSeydon und FindPOS.

Eine konventionelle Antiviren-Software bietet keinen umfassenden Schutz vor all diese Bedrohungen und durch die Einschränkungen, die sich bei Geldautomaten und POS-Systemen ergeben (schwache Kanäle, Low-End-Hardware und veraltete Software), gestaltet sich die Installation von Antiviren-Software oft kompliziert und unpraktisch. Daher können diese Viren täglich ungehindert die Geldautomaten und POS-Systeme von großen Finanzinstituten und Einzelhändlern angreifen und die Sicherheitssysteme umgehen.

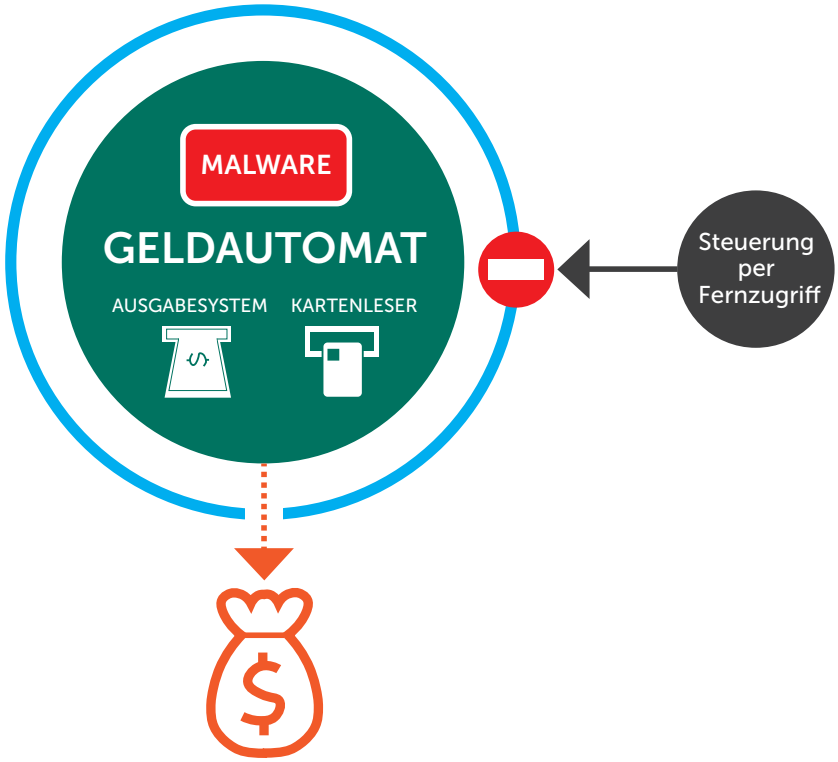
Cyberkriminelle dagegen verfügen über leistungsstarke und moderne Systeme, mit denen sie immer mehr zielgerichtete Malware für Geldautomaten und POS entwickeln.

Angriffsschema bei Geldautomaten

Geographisch verteilte Geldautomaten eignen sich ideal für die Infektion mit Malware als Teil eines zielgerichteten Angriffs, insbesondere, da USB-Anschlüsse und Tastaturen leicht zugänglich in einem Systemwartungsfach an der Rückseite des Geldautomaten untergebracht sind, das lediglich durch ein einfaches Schloss gesichert ist.

Womöglich ist das Schloss selbst noch nicht einmal ein Problem. Es ist keineswegs unüblich, dass Wartungsmitarbeiter vor Ort ein semi-permanentes USB- oder LAN-Modem bzw. -Kabel 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 geeignet, da die Wartungsmitarbeiter diese regelmäßig für die Wartung 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 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.

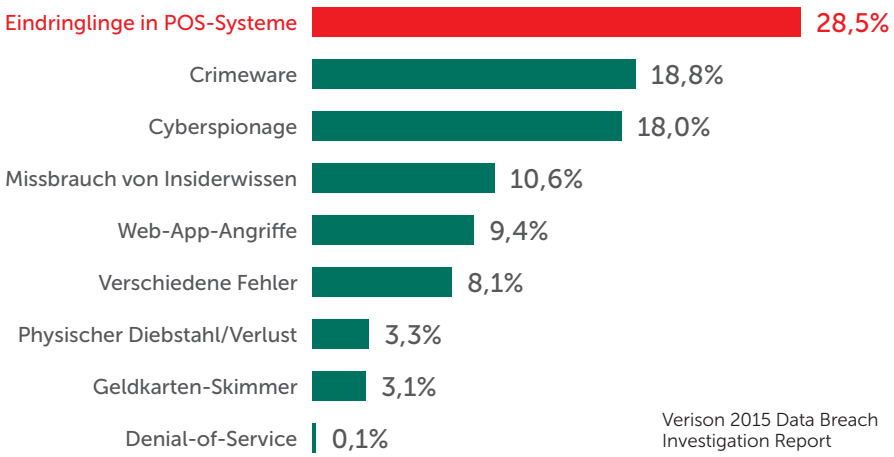


Mit einem einfachen Angriff auf Geldautomaten kommt man schnell und unkompliziert an echtes Geld. Infizierte Geldautomaten können jedoch auch Teil eines größeren Angriffsszenarios sein. Im Jahr 2015 wurde uns mit Carbank demonstriert, wie APT-Angriffe (Advanced Persistent Threat) zu finanziellen Verlusten führen können, die sich weltweit auf mehr als 1 Milliarde US-Dollar belaufen.

POS-basierte Bedrohungen

Häufigkeit von IT-Sicherheitsvorfällen

Klassifizierung der bestätigten Datendiebstähle



Verison 2015 Data Breach Investigation Report

Default Deny

Die meisten herkömmlichen Antiviren-Lösungen können vor diesen hochentwickelten, zielgerichteten Malware-Bedrohungen, denen sich die Branche gegenüber sieht, nicht ausreichend schützen. Die Default-Deny-Funktionalität bedient sich eines anderen, grundlegenderen Ansatzes. Keine ausführbaren Dateien, Laufwerke und Bibliotheken außer dem Softwareschutz können ohne Genehmigung des Sicherheitsadministrators auf einem Geldautomaten oder POS-Endpoint betrieben werden.

Gerätekontrolle

Mit der Gerätekontrolle von Kaspersky Lab können Sie USB-Speichergeräte kontrollieren, die mit der Hardware des Systems verbunden werden sollen, um so den Zugriff auf Geldautomaten oder POS-Systeme durch ein nicht genehmigtes Gerät zu verhindern. Somit werden diese anfälligen Systemeintrittspunkte blockiert, die regelmäßig von Cyberkriminellen bei Malware-Attacken als erster Schritt genutzt werden.

Geeignet für Windows XP – Windows 10 IoT

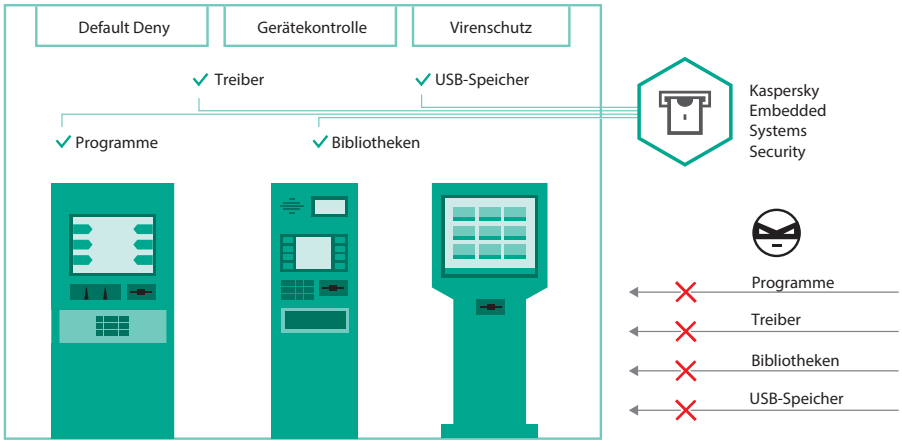
Nach zwölf Jahren lief im Januar 2016 der Support für Windows XP Embedded und im April 2016 der für Windows Embedded for Point of Service aus. Für das Betriebssystem Windows XP wird es keine weiteren Sicherheits-Updates und auch keinen technischen Support mehr geben. Kaspersky Embedded Systems Security bietet eine 100%ige Unterstützung der Windows XP-Produktfamilie.

Entwickelt für Embedded Systems Hardware

Kaspersky Embedded Systems Security bietet auch für Low-End-Systeme, die nahezu für alle Geldautomaten und POS-Hardware genutzt werden, absolute Sicherheit. Für Windows XP sind lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte des Systems notwendig. Im „bedarfsabhängigen" Betriebsmodus nutzt das separat installierte Antiviren-Modul die Hardware-Ressourcen nur während der manuellen oder geplanten Scans.

Antivirus und Kaspersky Security Network

Das Regelwerk des PCI DSS legt fest, dass alle Systeme, die Kredit- oder Debitkartendaten verarbeiten, über einen Virenschutz verfügen müssen, der regelmäßig aktualisiert wird. Kaspersky Embedded Systems Security bietet einen wirksamen Virenschutz sowie regelmäßige automatische oder manuelle Updates der Malware-Signaturen, sobald diese erforderlich sind. Über die Hälfte aller auf Geldautomaten und POS-Systemen gefundenen Malware gelangt über Zero-Day-/Zero-Second-Exploits in das System. Deshalb empfiehlt Kaspersky Lab zudem den intelligenten Schutz, der auf der Wissensdatenbank des Kaspersky Security Network basiert, um auf Exploits basierende Sicherheitsrisiken zu verhindern und abzumildern sowie die Reaktionszeit zu verkürzen.



Ein klassischer Schwachpunkt bei Point-Of-Sale-Systemen ist die Middleware, auf der sie basieren. Diese Middleware wird meist von kleinen Drittanbietern oder von internen Abteilungen entwickelt. Bei der Entwicklung spielt hierbei Funktionalität oft eine wichtigere Rolle als Sicherheit, und wie bei Geldautomaten wird ein einfacher Zugriff auf USB-Anschlüsse und CD-/DVD-Laufwerke als praktisch und weniger als Sicherheitsschwachstelle empfunden.

Die meisten POS-Systeme verarbeiten Kredit-/Debitkarten und unterliegen daher, wie auch Geldautomaten, dem PCI DSS-Standard. Ohne Ausnahme verarbeiten alle Systeme personenbezogene Kundendaten. Für den Schutz dieser Daten ist der Eigentümer des POS-Systems verantwortlich. Ferner sind alle POS mit einem Intranet verbunden, wodurch sie zu einem brauchbaren Eintrittspunkt für einen zielgerichteten Angriff werden.

Kaspersky Embedded Systems Security

Kaspersky Lab hat eine Sicherheitslösung entwickelt, die sich speziell an Unternehmen richtet, die Geldautomaten und POS-Systeme betreiben, und die entsprechende Bedrohungsumgebung einbezieht. Hierbei werden die einzigartige Funktionalität und das Betriebssystem, der Kanal sowie die Hardware-Anforderungen berücksichtigt, während Windows XP vollständig unterstützt wird.

Kaspersky Embedded Systems Security verringert die Sicherheitsrisiken, die typisch für Embedded Systems sind. Die Lösung wurde speziell für Geldautomaten und POS-Systeme entwickelt und schützt die für diese Architekturen typischen Angriffsflächen, während gleichzeitig entsprechende Hardware- und Effizienz-Aspekte berücksichtigt werden. Eine einzige intuitive Konsole bietet die Kontrolle und Transparenz, die Sie benötigen, um eine effiziente, mehrstufige Sicherheitslösung für Ihre Endpoints, unerlässlichen Systeme und die gesamte IT-Infrastruktur zu verwalten.

Die Implementierung von Default Deny für Anwendungen, Laufwerke und Bibliotheken sowie eine unterstützende Funktion zur Gerätekontrolle, ist der einzige Ansatz, mit dem die Sicherheit technisch veralteter Systeme gewährleistet werden kann, die sich weiterhin in Betrieb befinden.

Kaspersky Embedded Systems Security bietet einen „Nur Default Deny"-Betriebsmodus. Hinsichtlich der Systemanforderungen sind lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte notwendig – ideal für Systeme, die auf Windows XP basieren und mit Low-End-Hardware betrieben werden. Bedarfsabhängige Scans werden durch ein optionales Antiviren-Modul über das Kaspersky Security Network bereitgestellt, das auch die Möglichkeit des Patch Managements bietet.

Daher erfüllt diese Einzellösung drei verschiedene Kriterien:

- Effiziente Sicherung von schwierig zu verwaltenden Systemen
- Einhaltung der PCI DSS-Anforderungen 5.1, 5.1.1, 5.2, 5.3 und 6.2
- Ermöglichen einer weichen Zeitplanung für den Ersatz veralteter Systeme und Hardware

Konformität mit PCI DSS

Kaspersky Security für Embedded Systems erfüllt und übertrifft alle in den Unterpunkten von PCI DSS v3.2 festgelegten Sicherheitsstandards:

1.4: Installation persönlicher Firewall-Software auf allen tragbaren Computern, die außerhalb des Netzwerks eine Verbindung mit dem Internet herstellen und die auch für den Zugriff auf das CDE verwendet werden.

2.4a: Ein Inventar der Systemkomponenten führen, die für PCI DSS infrage kommen.

5.1: Auf allen Systemen, die am häufigsten von schädlicher Software betroffen sind (insbesondere PCs und Server), muss eine Antiviren-Software installiert werden.

5.1.1: Das Virenschutzprogramm muss alle bekannten Arten von schädlicher Software erkennen, entfernen und vor diesen schützen können.

5.2: Alle Virenschutzmechanismen müssen auf dem neuesten Stand sein, es müssen regelmäßig Scans durchgeführt und Audit-Logs generiert werden, die in Übereinstimmung mit Anforderung 10.1 des PCI DSS aufbewahrt werden müssen.

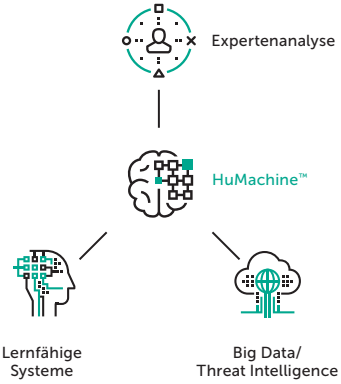
5.3: Es muss sichergestellt sein, dass die Virenschutzmechanismen aktiv ausgeführt werden und vom Benutzer nicht deaktiviert oder verändert werden können, wenn dies nicht explizit durch das Management von Fall zu Fall für eine begrenzte Zeit genehmigt wurde.

6.2: Alle Systemkomponenten und Software müssen vor bekannten Sicherheitslücken geschützt werden, indem die vom Hersteller bereitgestellten Sicherheitspatches installiert werden. Sicherheitspatches müssen innerhalb eines Monats nach Veröffentlichung installiert werden.

Mehr als nur Virenschutz

Der Payment Card Industry Data Security Standard (PCI DSS) reguliert viele der technischen Anforderungen und Einstellungen für Systeme zur Abwicklung von Kreditkartentransaktionen. Die Sicherheitsvorschriften für Geldautomaten und POS-Systeme scheinen jedoch nur den Virenschutz abzudecken. Wie oben bereits erwähnt, und wie bei aktuellen Angriffen deutlich wurde, ist ein rein auf Virenschutz basierender Ansatz im Fall der derzeitigen Bedrohungen von Geldautomaten und POS-Systemen jedoch nur von eingeschränkter Wirkung. Die Zeit ist gekommen, Gerätekontrolle und Default Deny auf Ihre unerlässlichen Embedded Systems anzuwenden, da diese sich bereits in anderen Sicherheitskontexten bewährt haben.

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



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise-security**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **www.kaspersky.de/blog/b2b**

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber. Lotus und Domino sind Marken von International Business Machines Corporation und als solche in vielen Rechtsgebieten weltweit eingetragen. Linux ist eine eingetragene Marke von Linus Torvalds in den USA und anderen Ländern. Google ist eine eingetragene Marke von Google, Inc.