BIOS-Erweiterung verhindert unbefugte Nutzung von Embedded-Systemen

Sicherheit im BIOS verankert

Klassisch betrachtet stellt das BIOS dem Betriebssystem eine virtualisierte Ansicht der Hardware zur Verfügung. Für die ersten digitalen Geräte auf PC-Basis reichte diese auf das Hochfahren der Hardware beschränkte Funktion aus. In vernetzten Betriebs-Umgebungen bietet dies allerdings Angriffspunkte für die unbefugte Nutzung von Rechnern und Netzen. *Core System Software* schafft hier Abhilfe und gewährleistet einen sicheren Betrieb von Embedded-Systemen in vernetzten Umgebungen.

Eine zunehmende Vernetzung vieler unterschiedlicher Geräte und das Speichern zahlreicher kritischer Daten in verteilten Anwendungen wirft immer stärker die Frage nach der Datensicherheit und der Vermeidung von unbefugten Zugriffen auf Daten und Netze auf. Wenn das Sicherheitsnetz keine Löcher aufweisen soll, dann muss bereits beim Booten eines Embedded-Systems die Grundlage für einen sicheren Betrieb im Stand-Alone- und vernetztem Betrieb gelegt werden – und zwar durch ein erweitertes BIOS. Diese *Core System Software* übernimmt damit Aufgaben, die über die Funktion des traditionellen BIOS weit hinausreichen.

BIOS: Aufgaben und Sicherheitslücken

Die Hauptfunktion des BIOS liegt bei konventionellen PC-Architekturen im Vorbereiten der Hardware für das Betriebssystem. Dazu werden ein Power On Self Test (POST) durchgeführt, die installierten Geräte hochgefahren, die Peripherie und Schnittstellen geprüft sowie das Betriebssystem geladen und gestartet. Seit der hohe Leistungsverbrauch von Rechnern und Peripheriegeräten in das Bewusstsein der Verbraucher vorgedrungen ist, umfasst das Aufgabengebiet des BIOS auch die Verwaltung der Energiespar-Optionen. Gefördert durch die zunehmende Vernetzung der Geräte und durch immer kürzere Lebenszyklen setzt die PC-Industrie vermehrt auf Flash-Speicher statt auf EPROMs zum Ablegen der Firmware. Dadurch wird eine Aktualisierung des BIOS mit Hilfe von Software-Routinen auch über das Netzwerk möglich ohne das Gerät öffnen und die Speicherkomponente austauschen zu müssen. Dem gesteigertem Komfort und der höheren Flexibilität des Systems steht aber ein entscheidender Nachteil gegenüber: Unbefugte können vergleichsweise einfach und unbemerkt die Firmware ändern. Der Zugriff auf das BIOS und das Beschreiben des Flash-Speichers ist dabei ausschließlich über Passwörter geschützt. Im Falle der Firmware existieren darüber hinaus in der Regel Master-Passwörter, die einen Missbrauch noch vereinfachen.

Auch der Zugriff auf ein Gerät und die Einwahl in ein Netzwerk sind meist nur durch ein Passwort und eine Benutzerkennung geschützt. Dem Betreiber der Anwendung bzw. des Netzwerks bleibt nur die Hoffnung, dass es sich bei demjenigen, der das Passwort eingibt, auch um die Person handelt, die die Befugnis zur Nutzung des Netzes hat. Für den Betreiber besteht keine Möglichkeit zu prüfen und zu kontrollieren, ob der sich einwählende PC von einem Virus befallen ist, anderweitig manipuliert wurde oder schlicht durch ein Versehen in unzulässiger Weise verändert wurde.

Gerade im Falle (vernetzter) Embedded-Systeme, die sensitive Daten akquirieren und zudem häufig für wechselnde Benutzer gedacht sind (zum Beispiel ein Verkaufsautomat oder Industriecomputer), stellen diese Sicherheitslücken eine große Gefahr dar.

Schutz sensitiver Daten und Vermeidung unbefugter Benutzung

Gerade bei Embedded-Geräten aus den Bereichen Messdaten-Erfassung, Prozess-Steuerung oder Sicherheit ist die Vertrau-

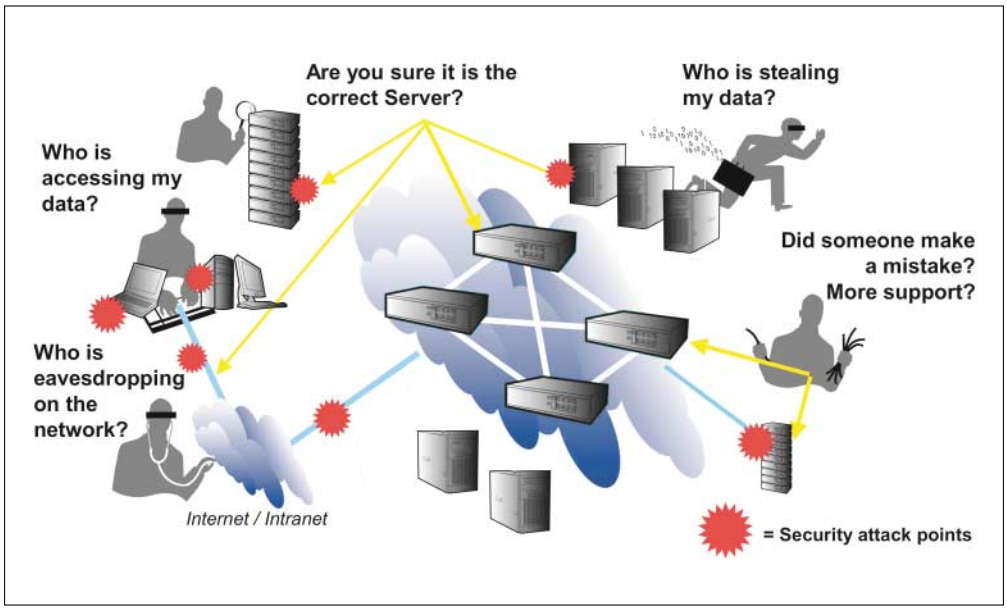

Bild 1: Angriffspunkte für unbefugte Benutzung in einem Netzwerk.

AUTOR

Lori Grob arbeitet als Product Manager Embedded Product Lines bei Phoenix Technologies.

KOMPAKT

Die Core System Software *Trusted Core Embedded* von Phoenix Technologies ermöglicht mit zusätzlichen Sicherheits-Funktionen eine nahtlose ‚Chain of Trust' (etwa: Vertrauens-Kette) beim Betrieb vernetzter und autonomer Embedded-Systeme auf x86-Basis.

enswürdigkeit häufig von entscheidender Bedeutung. Die geforderte Vertrauenswürdigkeit kann durch konventionelle Maßnahmen wie Passwörter nur unzureichend gewährleistet werden. Gleichzeitig unterliegen Embedded-Systeme häufig keiner Kontrolle durch den Betreiber oder Hersteller, da sie in der Regel dezentral eingesetzt werden. Erst eine Authentifizierung der Geräte erhöht den Schutz gegen Unbefugte oder versehentliches Verändern der Geräte.

Phoenix Technologies bietet dafür Software, mit der die Integrität der Firmware und des Betriebssystems geprüft und z. B. festgestellt werden kann, ob ein Virus die

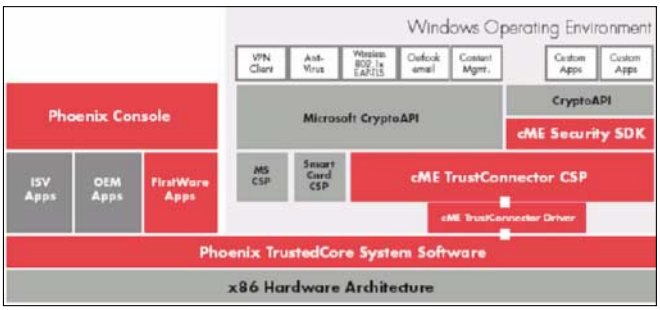

Bild 2: Die Architektur der Core System Software von Phoenix.

Software modifiziert hat. Auch wenn es kaum Viren geben wird, die die Firmware direkt angreifen, wird es häufiger vorkommen, dass befugte oder unbefugte Benutzer ein Gerät für eine andere Aufgabe als die vorgesehene verwenden wollen und dafür die Software bzw. die Firmware ändern. Digital signierte Updates der Core System Software sowie ein abgesicherter Flash-Speicher schützen das Herzstück des Systems vor Hacker-Angriffen und unbeabsichtigten Änderungen. Nur mit Hilfe der Anwendung ‚SecureFlash', die Windows- oder Linux-Systeme unterstützt, kann dann eine Änderung des Flash-Speichers vorgenommen werden.

Zur nahtlosen Geräte-Authentifizierung stellt Phoenix ein integriertes Kryptographie-Modul für den öffentlichen Schlüssel sowie einen Speicher für den sicheren Schlüssel bereit. Damit können sich das Gerät und das Betriebssystem gegenüber dem Netzwerk oder der Anwendung authentifizieren.

Die Core System Software nutzt dazu die enge Anbindung an die Hardware und legt den Schlüssel in einem Bereich ab, auf den das Betriebssystem keinen Zugriff hat. So kann sichergestellt werden, dass niemand den vorgegebenen (sicheren) Weg neu definiert, indem der Flash-Speicher neu beschrieben wird oder unerwünschte Modifikationen der Hard- und Software vorgenommen werden.

Ergänzung zu Firewall und Co.

Firewalls verhindern in vielen Fällen effektiv eine Bedrohung von außen. Wenn die Ursache für das Problem allerdings innerhalb der Firewall liegt, stößt sie schnell an ihre Grenzen: Wird das richtige Passwort eingegeben, steht das Netzwerk offen und zwar unabhängig davon, ob das Gerät infiziert ist oder für einen Zugang vorgesehen ist.

Eine Token-Karte und der Token-Schlüssel authentifizieren den Anwender und nicht das Gerät. In vielen Organisationen stehen Personen unterschiedliche Wege zum Zugriff auf das Netzwerk offen. Wenn sich ein Mitarbeiter z. B. mit einem Firmen-Laptop einwählt, dann weiß die IT-Abteilung hoffentlich, welchen Status die Antivirus-Software hat.

Verwendet der Mitarbeiter aber den Rechner eines Verwandten oder ein anderes, eventuell infiziertes Gerät, dann sind der Token-Schlüssel oder die Firewall wirkungslos.

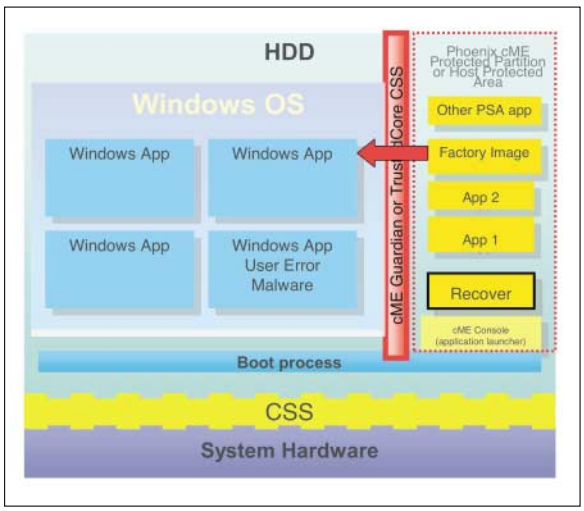

Bild 3: Die Wiederherstellungsfunktion Phoenix FirstWare Recover.

In der Embedded-Welt mit den dort üblichen vielen Benutzern pro Gerät wird es häufig nur das Gerät sein, das authentifiziert werden soll. In Sicherheits-Anwendungen wird es vielmehr darum gehen, das Gerät selbst zu schützen und eine absichtliche oder unabsichtliche Änderung des Systems zu erkennen bzw. zu verhindern.

Bei Medizintechnik-Anwendungen ist es zum Beispiel wichtig, dass die durch eine zuständige Stelle zertifizierte Stack-Konfiguration erhalten bleibt und nicht versehentlich durch das Installieren eines Patches verloren geht.

Eine Authentifizierung der Hard- und Software gibt Unternehmen zudem eine Methode in die Hand, nur bestimmte Betriebssysteme für den Zugriff auf das Firmennetzwerk zuzulassen – bisher sind sie auf den guten Willen und das Know-how der Anwender angewiesen.

Darüber hinaus kann Software für ganz bestimmte Geräte lizenziert werden. Dem Kopieren auf andere Systeme wird so wirksam ein Riegel vorgeschoben.

Diese Überlegungen zeigen, dass im Falle vernetzter Embedded-Systeme (die meist in organisationsinternen Netzen verknüpft sind) ein Schutz mit Firewalls, Passwörtern und Co. nicht ausreicht. Die Produkte von Phoenix sind komplementäre Elemente zu diesen Schutzmechanismen, die das Sicherheitsnetz wirksam abdichten.

Sichere System-Wiederherstellung

Quality of Service und Zuverlässigkeit sind beeinträchtigt, wenn die Gefahr besteht, dass Daten verloren gehen oder das Gerät angegriffen wird. Um dadurch verursachte Engpässe in anfälligen Netzen zu vermeiden, müssen ▶

mehr Geräte installiert werden, um eine gleich bleibende Leistung sicherzustellen.
Bei Einzelplatz-Rechnern oder Laptops ist der Datenverlust meist nicht so problematisch, da bei Ausfall einzelner Geräte die Produktivität der Gesamtorganisation nicht negativ beeinträchtigt ist – auch wenn der Verlust von Daten auch in diesen Fällen extrem unangenehm ist. Teuer oder gar lebensgefährlich dagegen wird es, wenn Embedded-Syteme ausfallen, die z. B. seltene oder sicherheitsrelevante Daten sammeln.
Eine zuverlässige Systemherstellungs-Funktion kann hier hohe Folgekosten vermeiden helfen, wie folgendes Beispiel zeigt: In Datenerfassungsanwendungen kommen häufig Embedded-x86-Systeme für die Akquisition komplexer Signale zum Einsatz (gegebenenfalls über lange Zeiträume hinweg wie z. B. in Umweltüberwachungs-Messtellen). Kommt es zu einem Datenverlust, muss der gesamte Test erneut durchlaufen werden. Zur Vermeidung dieses Problems bietet Phoenix eine Recovery-Anwendung, die für das Wiederherstellen von Embedded-Devices verwendet werden kann. Unternehmen wie National Instruments oder LeCroy haben den Vorteil dieser Funktion erkannt und diese bereits in aktuelle Produkte integriert.
Das vollständige System (einschließlich Betriebssystem, Anwendungen, Benutzerdaten, Arbeitsplatz-Einstellungen, Treiber etc.) wird dabei in einer dem Betriebssystem nicht zugänglichen Partition des Festplatten-Laufwerks in komprimierter Form abgelegt. Für 100 GByte Daten muss diese Partition etwa 50 GByte groß sein.

Breite Unterstützung von Embedded Systemen

Da sich die Charakteristika vernetzter Geräte stark unterscheiden und diverse Prozessoren zum Einsatz kommen, bietet Phoenix im Rahmen der *Trusted-Core*-Familie speziell zugeschnittene Core-System-Software für Notebooks, Desktops, Server und seit September 2004 auch *Trusted Core Embedded* für Embedded-Geräte an.
Die Palette der durch *Trusted Core Embedded* unterstützen Geräte ist breit definiert, da unter dem Begriff *Embedded-Systeme* Geräte wie in Polizeifahrzeugen installierte Notebooks, Oszilloskope, Point-of-Sale-Applikation oder auch Drucker und Industrie-PCs zusammengefasst werden. Bei *Trusted Core Embedded* handelt es sich daher in weiten Teilen um ein Superset der Merkmale der anderen Familienmitglieder.

Implementierung

Europäische OEMs, die sich über sichere und vertrauenswürdige Produkte unterscheiden wollen, können entweder ein Board/Modul kaufen, das Trusted Core unterstützt, oder selbst entsprechend spezifizierte Produkte entwickeln sowie auch einen der zahlreichen Partner von Phoenix in Europa beauftragen.
In der Regel wird es für den OEM Sinn machen, die Anpassung der Firmware durch einen der Phoenix-Partner durchführen zu lassen. In einigen wenigen Fällen wird auch die Modifikation der Software in eigener Regie Sinn machen, für die dann eine Quellcodelizenz erforderlich ist. Darüber hinaus gibt es Tools, mit denen auch Nicht-Bios-Experten bzw. Kunden ohne Quellcode-Lizenz in gewissem Rahmen die Core System Software anpassen können.

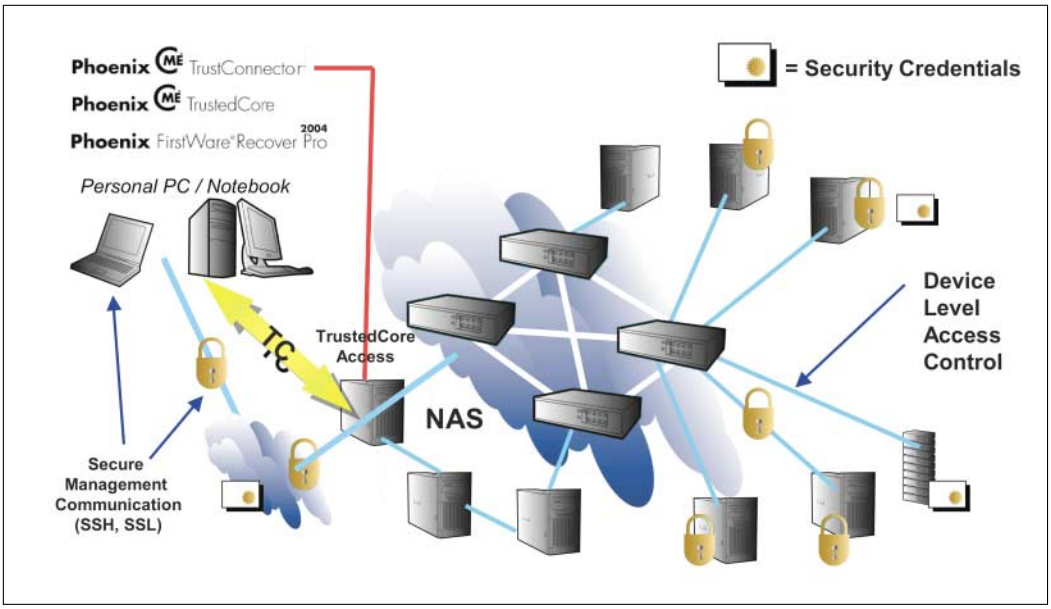

Bild 4: Mit Hilfe der Phoenix-Technologie lässt sich ein Netzwerk mit sicheren Endpunkten aufbauen.

Fazit

Heute wissen die Netzbetreiber kaum etwas über das Gerät, mit dem auf (interne) Netze zugegriffen wird. Sie hoffen, dass der Anwender auch der zugelassene Anwender ist.
Trusted Core Embedded, die Core System Software von Phoenix Technologies für vernetzte Embedded-Geräte, bietet zusammen mit der grafischen Entwicklungsumgebung *Core Architect* integrierte Sicherheit und Geräte-Authentifizierung für OEMs und ODMs.
Davon können gerade Deutschlands Hersteller hochwertiger Produkte profitieren und sich mit Hilfe vertrauenswürdiger Produkte auf dem Weltmarkt hervortun. Vor allem im Industriebereich, in dem verstärkt x86-Architekturen zu finden sind, ist es Zeit, zu handeln. Mit Hilfe moderner Core System Software können Status und Integrität der Geräte geprüft und die Basis für einen sicheren Betrieb von Netzwerken gelegt werden. (av)

KONTAKT

Phoenix Technologies Kennziffer 312
www.phoenix.com