April 2013

SecurityUPDATE

The MARX® Software Security Newsletter

www.marx.com

Sichere Zukunft oder Zukunft der Sicherheit

“Schöne neue Welt” war gestern. Nun brauchen wir die “Sichere neue Welt”. Früher liess Shakespeare seine Geister in die Schlacht ziehen, was Aldous Huxley zum gleichnamigen Buch inspirierte. Heute sieht Q die weltweite IT-Infrastruktur als das eigentlich zeitgemäße Schlachtfeld der Geheimdienste an. Sie nutzt uns allen, sie kann aber auch gegen uns verwendet werden.

Sicherheit wird weltweit nicht einheitlich definiert und interpretiert. Während sich in Deutschland aus mittlerer Vergangenheit noch Ressentiments gegen Überwachung, Blockwarte und den “gläsernen Menschen” regen, wird in USA der Zugriff und die Vermarktung privater Daten gesellschaftlich akzeptiert. Und von Softwaregiganten auch weidlich ausgenutzt. In anderen Gegenden der Welt sind staatliche Überwachungsmaßnahmen die Regel. Die Neugier mancher Staaten und krimineller Kartelle macht vor der deutschen Grenzkontrolle nicht halt.

Die vernetzte Informationsgesellschaft wird in Zukunft schwer abzuschätzenden Risiken ausgesetzt sein. Wieviel Transparenz wird uns aufgezwungen werden? Wem überlässt man die Kontrolle? Wiederholt sich immer alles? Man sollte mal wieder einen dystopischen Roman zur Hand nehmen und sich seine eigenen Gedanken machen.

RM

Lizenzsicherung in der Cloud oder lokal: was ist die bessere Lösung?

Wie sichert man als Softwarentwickler oder Anbieter seine Investitionen ab, wenn man neue Technologien wie Cloud Computing oder den Einsatz von mobilen Geräten berücksichtigt? Gerade bei teuren Anwendungen im Industrieumfeld möchte man sich nicht nur auf die Standard-Sicherheitsfeatures der Geräte- oder Appstore-Anbieter verlassen.

Cloud Computing liegt im Trend. IT-Infrastruktur wird nicht mehr selbst bereitgestellt und gewartet, sondern die benötigten Ressourcen, wie Speicherplatz und webbasierte Anwendungen, werden von den entsprechenden Anbietern einfach online gemietet. Die Vorteile liegen auf der Hand: man braucht sich selbst nicht um die Anschaffung und Wartung von Hard- und Software zu kümmern, das übernimmt der Anbieter. Ausserdem kann man bequem von überall auf die Dienste zugreifen, egal ob vom Computer in der Firma, oder vom Tablet/Laptop unterwegs.

Dennoch hat die Bereitstellung von klassischen Anwendungen direkt vor Ort ebenso ihre Daseinsberechtigung. Als ein wichtiger Punkt ist hier zum Beispiel die Ausfallsicherheit zu nennen. So ist die Anforderung bei viele Mission-Critical-Anwendungen, dass sie auch bei Strom- und Netzwerkausfall weiterlaufen. Ein weiteres Thema ist die Vertraulichkeit wichtiger Daten. Informationen und Daten über Produktentwicklungen oder auch Produktionstechniken dürfen beispielsweise keinesfalls

In dieser Ausgabe

die Abteilung verlassen. Oder das zu schützende System hat aus Sicherheitsgründen keine Netzwerkverbindung, bzw. am Standort ist keine verfügbar. Nicht zuletzt lässt sich beim Hosten von Anwendungen und Daten in der Cloud - oft im Ausland - nur schwer kontrollieren wer alles Zugriff darauf hat.

Es hängt daher vom jeweiligen Anwendungsfall ab, für welche Lösung man sich entscheidet. Der wichtige Punkt für den Softwareanbieter ist jedoch in beiden Fällen: wie stelle ich sicher, dass ich jede Lizenz bezahlt bekomme? Das CRYPTO-BOX System ermöglicht in beiden Fällen eine sicheres und zuverlässiges Lizenzmanagement.

Beispiel Cloud Computing:
Mit Smarx Cloud Security (WEB API) ist der Zugriff auf Webanwendungen nur mit der CRYPTO-BOX möglich. Diese befindet sich entweder direkt am Computer, oder an einem beliebigen Computer oder Server im Netzwerk. Damit ist auch eine einfache Lizenzierung für mobile Geräte wie Tablets oder Smartphones möglich. Die in der CRYPTO-BOX gespeicherten Informationen bestimmen, welche Lizenzrechte dem Benutzer eingeräumt werden. Der Softwareanbieter hat ausserdem die Möglichkeit, die CRYPTO-BOX auf demselben Weg jederzeit zu aktualisieren und mit Lizenzerweiterungen und Upgrades Geld zu verdienen.
Zusätzlich besteht die Möglichkeit, eine Lizenz an eine bestimmte Hardware zu binden. So kann man beispielsweise den Betrieb einer internen Software auf das Unternehmen beschränken - ein wichtiges Sicherheitsfeature.
Die Client-Komponente ist für alle gängigen Browser verfügbar, für die Serverseite Bibliotheken und als Beispielcode auf Basis von PHP.

Weitere Details zu Smarx Cloud Security erhalten Sie in dem Entwickler-Tip in diesem Newsletter.

Beispiel Schutz klassischer Anwendungen:
Hier stellt die CRYPTO-BOX vor Ort beim Endanwender sicher, dass nur bezahlte Lizenzen eingesetzt werden können. Die CRYPTO-BOX kann lokal am PC oder Laptop angeschlossen werden und sichert so die Lizenz auf diesem Gerät. Bei Einsatz im Netzwerk lassen sich Softwarelizenzen gleich auf mehreren Arbeitsstationen absichern, sowie auf mobilen Geräten. Über Remote Update können weitere Lizenzen oder Features freigeschaltet werden.

Bibliotheken und Beispielcode sind für alle gängigen Entwicklungsumgebungen unter Windows, Linux, Mac OS X, iOS und Android erhältlich.

Herausforderung "Integrated Industry"
Schutz von Produktions-Knowhow und Lizenzen

Das Leitthema der Hannover Messe 2013 lautet "Integrated Industry" und trägt der Vernetzung und intelligenten Steuerung von industriellen Anlagen Rechnung.

Die industrielle IT wächst immer mehr mit anderen Bereichen wie Business- und Kommunikations-IT zusammen. Es werden zunehmend ähnliche Hardware und gemeinsame Kommunikationsnetze eingesetzt. Standard PC-Technik, Tablet-PCs und Smartphones dienen als Bedien- und Kontrollpanels. Die umfangreiche Kontrolle über Produktionsprozesse ermöglicht mehr Effizienz und Flexibilität, birgt aber auch mehr Risiken.
Damit ergeben sich für Hersteller von Steuerungssoftware für Produktionsanlagen ähnliche Herausforderungen wie bisher für Software Distributoren in anderen Bereichen.

Wie kann sichergestellt werden, dass die Lizenzbedingungen eingehalten werden? Wie können Mehrfachnutzung und die Verbreitung von unautorisierten Duplikaten verhindert werden? Wie kann Kopierschutz von Knowhow und Steuerungsabläufen gewährleistet werden? Und wie kann Hacking oder das Einschleusen von Trojanern und Sabotage-Programmen verhindert werden?

Als Neuheit stellt MARX auf der Hannovermesse mit CBWEB einen Lizenzserver in Form eines Minicomputers vor, der in ein bestehendes Netzwerk integriert werden kann. Mit dieser "Integrated Security" Lösung ist eine einfache Lizenzierung von Arbeitsplätzen im Netzwerk möglich. Weitere Lizenzen oder Features können jederzeit nachträglich freigeschaltet werden. Ein weiterer Vorteil der zentralen Lizenzverwaltung mit CBWEB ist die Sicherstellung, dass die Software nur innerhalb des Unternehmensnetzwerks ausgeführt werden kann

Zugriffsschutz für Anlagen und Steuerungssysteme ist ein weiterer Anwendungebereich des CRYPTO-BOX Systems im industriellen Umfeld. Mit der WEB API Erweiterung "Smarx Cloud Security", wird sichergestellt, dass nur autorisierte Nutzer und geschultes Servicepersonal Zugriff auf bestimmte Anlagen im Netzwerk haben. Voraussetzung ist, dass auf dem Zielsystem ein Webserver läuft.

MARX kann auf langjährige und erfolgreiche Erfahrung in der Entwicklung von Softwareschutz und Lizenzmanagement zurückblicken. Das CRYPTO-BOX System gewährleistet einen sicheren Lizenzschutz, sowohl am lokalen Computer als auch in Netzwerken. Unterstützt werden alle gängigen Entwicklungstools unter Windows (inkl. RT), Linux, iOS und Android. Kundenspezifische Anpassungen und die individuelle Integration des Schutzes in Kundensysteme können durch MARX realisiert werden. Die CRYPO-BOX ist EAL-zertifiziert und die Implementierung von Standard-Verschlüsselungsverfahren wie AES und RSA in der Hardware bieten Schutz gegen Auslesen und Duplizierung.

SPOTLIGHT

Treiberupdate für die CRYPTO-BOX

Für die CRYPTO-BOX XS und Versa steht ein aktualisiertes Treibersetup (CBUSetup.exe) zur Verfügung.
Es enthält einen Workaround für die inkorrekte Abarbeitung einiger CRYPTO-BOX Befehle durch den Intel USB 3.0 Treiber. Wir empfehlen daher den neuen CRYPTO-BOX Treiber auf allen Systeme mit USB 3.0 Ports zu installieren.

Unterstützung für Lizenzbindung

Das aktuelle Protection Kit enthält Beispielcode in C++ und C# (Visual Studio) zur Bindung der Software an einen bestimmten Computer, sowie mit dem aktuellen SmarxDemo ein GUI-basiertes Beispiel zur Veranschaulichung der Funktionalität.

Support für Embarcadero XE3

Bibliotheken und Beispiele zur Einbindung der CRYPTO-BOX unter Embarcadero XE3 (CBuilder und Delphi x64) sind im aktuellen Protection Kit 5.90 enthalten.

Download unter:
www.marx.com/downloads

Entwickler-Tip

Smarx Cloud Security (WEB API) 4.0 zur Benutzeridentifizierung und Aktualisierung der CRYPTO-BOX einsetzen

Smarx Cloud Security (WEB API) ist eine Erweiterung für das CRYPTO-BOX Schutzsystem. Es stellt sicher, dass nur authentisierte Nutzer Zugriff auf bestimmte Web-Inhalte oder Updates haben - sowohl im Intranet als auch im Internet.
Die Anwendungsbereiche sind vielfältig: Support nur für zahlende Kunden, Zugriff auf bestimmte Inhalte nur für autorisiertes Servicepersonal, und vieles mehr.

Smarx Cloud Security bietet folgende Möglichkeiten:

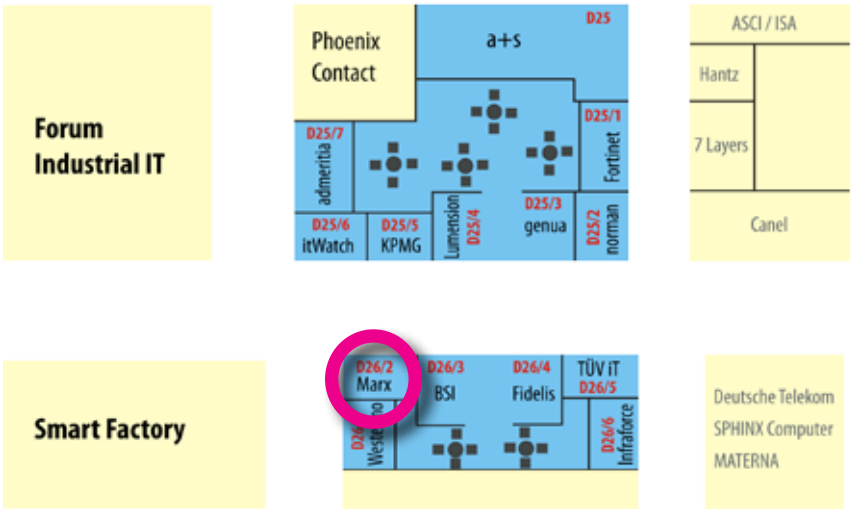
1. Zugriff auf Webinhalte nur mit der CRYPTO-BOX
Dieses Szenario eignet sich zum Beispiel dann, wenn Zugriff auf bestimmte Inhalte nur für berechtigte Anwender erlaubt werden soll. Beim Aufruf der Webseite wird die CRYPTO-BOX abgefragt, und je nach Status der Zugriff auf die Seite erlaubt oder verwehrt.

2. Aktualisierung der CRYPTO-BOX
Smarx Cloud Security kann ebenso zur Aktualisierung der CRYPTO-BOX beim Anwender eingesetzt werden. Im Gegensatz zu Remote Update entfällt hier das (manuelle) Versenden von Aktivierungskeys, der Vorgang läuft komplett automatisiert ab. Das eröffnet die Möglichkeit, rund um die Uhr Folgeumsätze zu generieren, beispielsweise für weitere Features oder Lizenzen. Mit Online License Management (OLM) können zusätzlich Update-Pläne für unterschiedliche Szenarien definiert werden.

Die aktuelle Version von WEB API wartet mit neuen Funktionen auf. So kann die CRYPTO-BOX sowohl lokal (direkt an Client angeschlossen) als auch über Netzwerk eingebunden werden. Auf diese Weise lassen sich beispielsweise mobile Geräte ohne USB-Anschluss wie Tablets oder Smartphones mit einbinden. Ein weiteres Feature ist die Unterstützung für Lizenzbindung an den Client. Ein mögliches Einsatzgebiet dafür ist, den Zugriff auf bestimmte Inhalte oder den Betrieb einer internen Software auf bestimmte Geräte zu beschränken.

Eine Demonstration von WEB API inkl. Lizenzbindung finden Sie auf unserer Webseite unter: www.marx.com/websec/new/

Hannover Messe 2013
Sie finden uns in Halle 8 Stand D26/2 auf dem Partnerstand von A+S



IMPRESSUM

MARX Software Security GmbH
Vohburger Strasse 68
D-85104 Wackerstein
Tel. +49(0)8403/9295–0
Fax +49(0)8403/1500
sales-de@marx.com
www.marx.com

Wir sind telefonisch für Sie auf der Messe erreichbar unter:
0163-1532063

0D11Mar13sa(SecurityUpdate).indd