

# SecurityUPDATE

The MARX® Software Security Newsletter

www.marx.com

## Der kleine Unterschied

Nein, ich will hier nicht über Dongles reden. Sondern über den kleinen Unterschied beim Umgang mit Computern. Es gibt ihn nämlich. Um festzustellen, ob Computer eher männlich oder eher weiblich sind, bildete ein Professor zwei Gruppen von Computer-Experten. Die erste bestand aus Frauen, die zweite aus Männern. Jede Gruppe wurde gefragt, welches Geschlecht sie einem Computer zuordnen würde und warum. Dies sollte mit drei Punkten begründet werden.

Die Gruppe der Frauen meinte, Computer wären typisch männlich:

1. Um ihre Aufmerksamkeit zu bekommen, muss man sie anmachen.
2. Sie haben eine Menge Daten, aber wissen trotzdem nichts.
3. Sie sollten eigentlich dabei helfen Probleme zu lösen, aber oft sind sie selbst das Problem.

Für die Männer waren Computer ganz klar weiblich, denn:

1. Keiner außer ihrem Schöpfer versteht ihre interne Logik.
2. Die Sprache, die sie untereinander benutzen, ist völlig unverständlich für andere.
3. Sogar kleinste Fehler bleiben für immer sicher gespeichert.

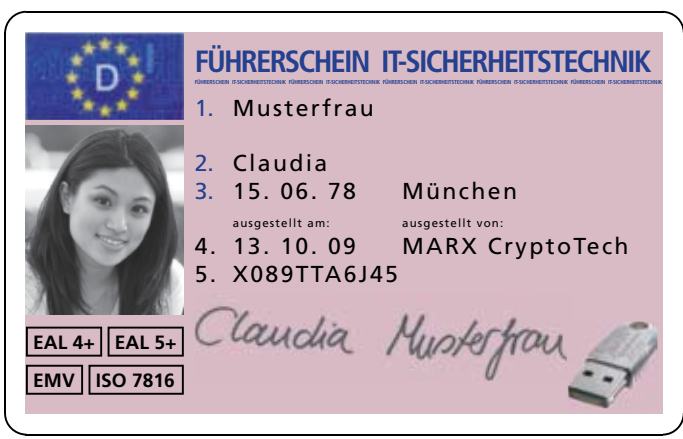
Warum diese Überlegungen? Es ist mir aufgefallen, dass es meist nur Männer sind, die den CryptToken bestellen. Woran liegt das? Weil er so männlich wirkt? Weil er von Männern für Männer gemacht wurde? Oder weil er weder bunt ist noch gut riecht? Nicht mal brilliant besetzt oder als Sammelobjekt geeignet? Auf Mädels, über Eure Ideen freuen wir uns: rmarx@marx.com.

Romy Marx

## Paradigmenwechsel beim Datenschutz

### Führerschein für IT-Sicherheit

Von der Druckerpresse bis hin zur weltweiten Vernetzung - im Rausch der Geschwindigkeit werden Mensch und Daten immer mehr gläsern. Hier kann nicht nur die Technologie den richtigen Schutz bieten, es muss bei der "Sicherheitserziehung" anfangen. Alte Denkmuster der Sorglosigkeit müssen durch Aufzeigen der realen Gefahren erkannt und überholt werden. Intelligente Identifikation und Geheimhaltung von vertraulichen Informationen ist nun mal vielschichtig und aufwendig. Vielleicht sollte man einen Führerschein für IT-Sicherheit einführen?



ein Paradigmenwechsel in der Informationstechnologie eingesetzt. Aber gilt dieser Wechsel auch für die Sicherheitstechnik? In der kurzen IT-Geschichte gab es bereits mehrere Wechsel von vorherrschenden Denkmustern.

Als die wichtigste Erfindung der letzten 2500 Jahre gilt die Druckerpresse. Nichts revolutionierte das Wissen unseres Kulturkreises so sehr, wie die Möglichkeit der raschen Verbreitung des geschriebenen Wortes. Der schnelle Austausch von Ideen, Erfindungen, Informationen und Ideologien verwandelte die Welt.

Wir leben im digitalen Zeitalter und seit der weltweiten Zugänglichkeit fast allen Wissens über Kleinstgeräte in unserer Hand, hat

Die Programmierung der ersten Computer war nur mit spezieller Kenntnis zu realisieren und die Sicherheit war vernachlässigbar.

Mit der Entwicklung höherer Programmiersprachen in den 70ern bekamen mehr Menschen Zugang zur Materie. Die Computer konnten nun Unmengen von Daten verarbeiten, aber die weltweite Vernetzung war noch vergleichsweise limitiert und bot eine gewisse Sicherheit durch Professionalität.

In dieser Ausgabe:	
Der kleine Unterschied .....	S.1
Führerschein für IT-Sicherheit ....	S.1
Sichere Benutzerauthentifizierung bei Webportalen .....	S.2
Flexibles Lizenzmanagement mit der CRYPTO-BOX .....	S.3
Spotlight: PPK 3.80 .....	S.3
Ins .NET gegangen .....	S.4

In den 80ern nahm die Verbreitung der - noch teuren - PCs für den Mittelstand und Privatbereich zu. Der Feind kam dabei meist von "innen". Mit mobilen Datenträgern konnten schnell Kundendaten an die Konkurrenz gelangen.

In den 90ern war die EDV-Gemeinde im Vergleich zu heute immer noch relativ sicher, da die Geräte nicht so mobil und kommunikativ waren. Viele Unternehmen waren mit Firewalls, etc. zwar nach aussen hin annähernd unangreifbar, aber nicht unbedingt gegen den "inneren Schweinehund". Denn schnell wanderte unbemerkt Vertrauliches auf Diskette oder CD aus dem Büro.

Der größte Paradigmenwechsel setzte zum Jahrhundertwechsel mit der weltweiten Vernetzung, preisgünstiger Hardware und mobilen Zusatzgeräten zum Datenaustausch ein. Die Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) beziffert den Schaden durch Industriespionage im Jahre 2008 auf ca. 30 Mrd. Euro allein in Deutschland.

Wie können wir uns auf immer billigere und leistungsstärkere Hardware verlassen, die oft auf überholten Sicherheitstechnologien basiert? Schneller Profit verwischt leicht ethische Bedenken. Nicht jeder Endanwender kann ein EDV-Sicherheitsexperte sein. Man sollte sich wie beim Auto darauf verlassen können, dass das gekaufte Vehikel einwandfrei funktioniert und die vom TÜV bestätigte Sicherheit bietet. Leider passiert immer noch genug, denn die größte Schwachstelle ist menschliches Fehlverhalten.

Gleiches gilt auch für IT-Sicherheit. Im Rausch der Geschwindigkeit werden mögliche Gefahren ausser Acht gelassen. Hier kann nicht nur die Technologie den richtigen Schutz bieten, auch alte Denkmuster müssen durch Aufzeigen der realen Gefahren erkannt und überholt werden. Sichere Authentifizierung und Identifikation verlangt mehr als Passwörter - vielleicht einen Führerschein für IT-Sicherheit?

**Cloud-Computing – wie wird´s sicher?**

## Eindeutige Benutzerauthentifizierung bei Webportalen und Online-Diensten

Die Vorteile und Chancen von Cloud-Computing sind unbestritten, aber die großen Herausforderungen, nämlich der sichere Datentransfer zwischen lokalem Client und entferntem Server und die eindeutige Benutzeridentifizierung, ziehen immer noch Risiken nach sich. Mit MARX WebSecurity lassen sich diese Risiken minimieren.

➤ In die gleiche Kerbe schlagen Modelle wie Software-Leasing oder „Software as Service“ (SaaS). Bei diesen Leistungen befinden sich die Anwendungen und Daten nicht mehr auf einem Firmenserver oder auf dem PC, sondern der Zugriff erfolgt extern. Diese „Auslagerung“ birgt die Gefahr des unberechtigten Zugriffs oder des Missbrauchs.

### Neue Modelle werden die IT-Landschaft gravierend ändern

Microsoft-Chef Steve Ballmer sieht in Cloud-Computing eines der zukünftigen, dominanten und zentralen Themen der Informationstechnologie. On-Demand-Software und Software-as-a-Service werden gravierende Veränderungen für Softwarehersteller nach sich ziehen und neue und hohe Anforderungen an professionelle Schutzstrategien und Lizenzlösungen stellen.

### Eindeutige Identifizierung der Benutzer durch WebSecurity

Mit der CRYPTO-BOX und dem WebSecurity Toolkit bietet MARX eine Lösung zur Minimierung dieser Risiken. Web API ermöglicht bei Internet/Intranet-basierten Anwendungen wie eBusiness-Lösungen, Finanz- und Bankdiensten oder Abonnementservices die eindeutige Identifizierung eines jeden Benutzers. Hersteller von Webanwendungen erhalten damit ein einfach zu handhabendes Werkzeug zur Integration einer sicheren, hardwarebasierten Authentifizierung auf Basis der CRYPTO-BOX in gängige Client-Server-Umgebungen.



Cloud Computing beschreibt ein Konzept, das die IT-Landschaft in allen seinen Bereichen verändern könnte. Programme, Anwendungen, etc. werden dabei nicht mehr selbst betrieben, sondern von extern - über das Internet - bezogen.

### Online-Vertrieb von Lizenzen mit der CRYPTO-BOX

MARX WebSecurity ermöglicht auch den Online-Vertrieb und die -Aktualisierung von Lizenzen. So können sowohl Lizenzmodelle auf Mitgliedschaftsbasis als auch kundenspezifische Lösungen realisiert werden, sodass nur autorisierte Benutzer mit der entsprechenden CRYPTO-BOX die erworbenen Leistungen oder abonnierten Dienste nutzen können.

Neben der einfachen Implementierung in bestehende Webportale und der Plattformunabhängigkeit auf der Serverseite bietet WebAPI einen optimalen Schutz gegen Phishing und Passwortschleichen sowie Zugangskontrolle für Intranet- und Internet-Dienste und -Anwendungen.

## Das CRYPTO-BOX Protection Kit 3.80

# Folgeumsätze und dauerhafte Kundenbindung durch flexibles Lizenzmanagement mit der CRYPTO-BOX

Das neue SmarxOS Protection Kit 3.80 wartet mit einem erweiterten System zum Lizenzmanagement auf. Mit Remote Update lassen sich nicht nur bestehende Datenobjekte in der CRYPTO-BOX aktualisieren, sondern es können auch neue Partitionen und Datenobjekte direkt beim Kunden angelegt werden. Das kann z.B. nützlich sein, wenn man nachträglich weitere Lizenzen hinzufügen möchte. Das ganze lässt sich ohne Programmieraufwand entweder über die Oberfläche des SmarxOS Application Frameworks (SxAF) oder das kommandozeilenbasierte RU-Tool.exe realisieren.

➤ Voraussetzung ist eine Lizenz von Remote Update, die durch eine einmalige Investition freigeschaltet werden kann, oder bei einer Bestellung von 100 CRYPTO-BOXen im Preis enthalten ist. Danach ist eine unbegrenzte Anzahl von Updatevorgängen möglich.

### Datenobjekte und Partitionen

Wurde die CRYPTO-BOX des Kunden bereits mit einem bestehenden SxAF-Projekt formatiert, kann das Update über die SxAF-Oberfläche durchgeführt werden. Dazu kann das Projekt um die gewünschten Partitionen und Datenobjekte erweitert werden. Anschließend wird der Remote Update Vorgang durchgeführt.

### RU-Tool und Kommandozeilen

Falls kein SxAF-Projekt vorhanden ist (z.B. weil die CRYPTO-BOX manuell konfiguriert wurde), ist ein Update über das kommandozeilenbasierte RU\_Tool.exe möglich.

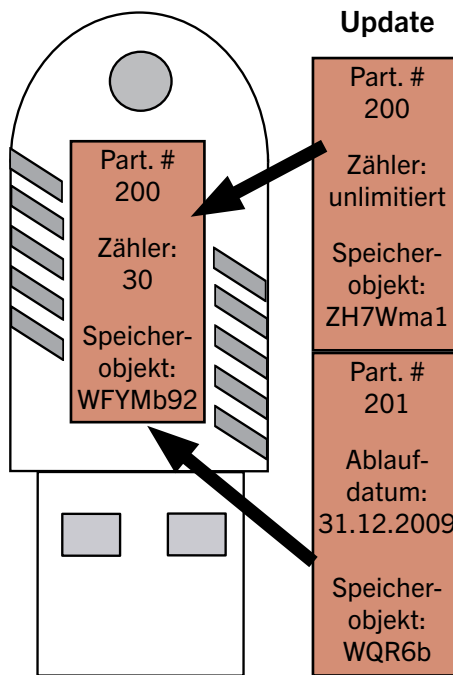
Beide Möglichkeiten werden in den Application Notes zu Remote Update erläutert. Diese stehen unter [www.marx.com/AN](http://www.marx.com/AN) zum Herunterladen zur Verfügung.

### Spotlight

Das aktuelle CRYPTO-BOX Protection Kit (PPK 3.80) steht zum Download bereit ([www.marx.com/downloads](http://www.marx.com/downloads)).

#### Beispiele für Delphi 2010:

MARX stellt Bibliotheken und Beispiele zur Einbindung der CRYPTO-BOX unter [www.marx.com/downloads](http://www.marx.com/downloads) zur Verfügung.



### Intelligente Formatierung

Eine weitere Neuerung betrifft die Formatierung: Bei den bisherigen Versionen des Protection Kits war es erforderlich, dass die CRYPTO-BOX bereits mit den passenden Partitionen vorkonfiguriert war, wenn die Optionen AutoCrypt (automatischer Softwarechutz), Document Protection, Netzwerk-Lizenzmanagement oder Remote Update genutzt wurden.

Ab dem Professional Protection Kit 3.80 ist dies nicht mehr notwendig, die Partitionen werden bei Bedarf automatisch beim Formatieren der CRYPTO-BOX erzeugt.

### Automatische Generierung von Partitionen

Generiert werden die Partitionen entweder über die grafische Oberfläche (SmarxOS Application Framework) oder über das Kommandozeilentool SmrxProg.exe.

Das CRYPTO-BOX Protection Kit erhalten alle Kunden kostenlos zusammen mit ihrer CRYPTO-BOX Bestellung. Die aktuelle Version ist unter [www.marx.com/downloads](http://www.marx.com/downloads) verfügbar.

### OLM und SOLO Server

Das Online License Management (OLM) bietet sich als flexible Alternative zu Remote Update an. Es ermöglicht eine automatische Aktualisierung von Lizenzen über einen Webserver anhand von Update-Skripten, eine manuelle Interaktion wie bei Remote Update ist nicht notwendig.

OLM empfiehlt sich daher besonders, wenn oft Updates benötigt werden und diese zu jedem Zeitpunkt möglich sein sollen.

Außerdem kann OLM mit Online-Abrechnungssystemen, z.B. SOLO Server, kombiniert werden.

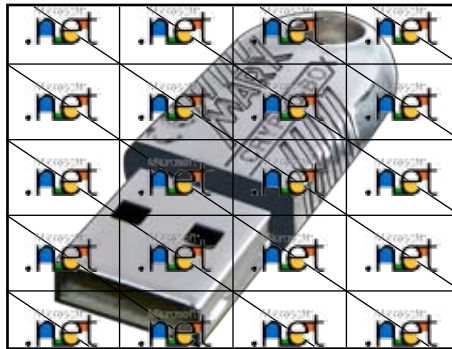
Weitere Informationen zu Online License Management erhalten Sie unter [www.marx.com/olm](http://www.marx.com/olm).

## Entwickler-Tips

### Ins .NET gegangen

Mit CBIOS4NET bietet MARX eine vollständig objektorientierte und komponentenbasierte Syntax für .NET-Entwickler. Diese unterstützt alle vorhandenen CRYPTO-BOX Schnittstellen.

➤ Viele .NET-Programmierer greifen auf dieses lauffzeit-basierte System zurück, weil Codierfehler stark vermindert werden. Mit CBIOS4NET bietet MARX den .NET-Entwicklern eine komponentenbasierte Syntax. Diese beinhaltet Klassen, die in Namensräume (Namespaces) unterteilt sind, und so den Zugriff auf alle CRYPTO-BOX Funktionen ermöglichen. Diese sind:



#### CBIOS CRYPTO-BOX Management

- Details & Status der CRYPTO-BOX
- Lesen & Schreiben von Daten
- Verschlüsselungsfunktionen
- Lizenzinformationen (Zähler, Ablaufdatum, etc.)
- Steuerung des CRYPTO-BOX Netzwerkservers

#### CBIOS.RFP Remote Update Management

- Aktualisierung der CRYPTO-BOX direkt beim End-User

#### CBIOS.DP

- Verschlüsselung von anwendungsspezifischen Daten

#### CBIOS4NET für 32- und 64 Bit Windows-Plattformen

Die CBIOS4NET Bibliothek ist sowohl in einer 32 Bit- als auch einer 64 Bit-Version verfügbar. Darüber hinaus stehen Beispiele mit nützlichen Anwendungsszenarien bereit:

- Ver-/Entschlüsseln von Assemblies
- Verschlüsselung digitaler Medien (Video/Audio) und größerer Datenmengen
- Administration des CBIOS Netzwerkservers

Unter [www.marx.com/downloads](http://www.marx.com/downloads) steht CBIOS4NET - als Teil des aktuellen Protection Kits - zum Download bereit.

Das Entwicklerkit können Sie unverbindlich testen: [www.marx.com/kit](http://www.marx.com/kit)

## Rätsel:

Finden Sie die unten dargestellten Wörter. Alle Laufrichtungen (senkrecht, waagrecht und vertikal) sind möglich. Schicken Sie uns Ihre Lösung und sichern Sie sich Ihre Chance auf den Gewinn eines iPod Shuffle.



Fax oder Email an: 08403/1500 oder [contact-de@marx.com](mailto:contact-de@marx.com)

Einsendeschluss: 31.10.2009

- Betreff: MARX Security Update - Rätsel
- Die Koordinaten von "MARX" lauten?
  - Die Koordinaten von "SOFTWARE" lauten?
  - Die Koordinaten von "SECURITY" lauten?
- Der Rechtsweg ist ausgeschlossen.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	R	X	T	H	A	R	D	W	A	R	E	A	N	I	B
b	E	D	R	M	A	U	S	A	I	Z	N	E	Z	I	L
c	V	A	O	I	D	U	A	D	T	N	W	U	X	Q	R
d	R	T	P	D	O	W	N	L	O	A	D	O	S	E	E
e	E	U	P	D	A	T	E	G	G	N	B	O	H	B	M
f	S	M	A	L	I	N	U	X	I	O	G	C	W	U	O
g	C	X	R	E	B	I	E	R	T	S	I	L	H	S	T
h	R	M	R	W	K	V	J	P	B	S	E	Q	E	I	E
i	Y	E	M	A	C	E	Y	O	K	E	F	R	A	M	P
j	P	T	H	R	M	R	D	R	A	C	T	R	A	M	S
k	T	I	B	E	C	S	O	T	L	U	M	I	W	S	C
l	O	S	Y	C	P	A	E	A	S	R	N	T	T	C	H
m	K	B	T	I	O	Q	D	S	W	I	B	S	F	A	U
n	E	E	E	P	C	L	I	E	N	T	S	A	O	P	T
o	N	W	S	A	J	A	V	A	J	Y	U	G	S	I	Z

AES	ITSA	SAFESIGN
API	JAVA	SCHUTZ
AUDIO	JCOP	SECURITY
BINAER	KEY	SERVER
BYTES	LINUX	SICHER
CEBIT	LIZENZ	SMARTCARD
CHIP	MARX	SOFTWARE
CLIENT	MAC	TREIBER
CRYPTOBOX	MAUS	TOKEN
CRYPTOKEN	MIDDLEWARE	UPDATE
DATA	MSCAPI	USB
DATUM	MULTOS	VERSA
DONGLE	NETZ	VIDEO
DOWNLOAD	RAPPORT	WEBSITE
EMAIL	REMOTE	WINDOWS
HARDWARE	RSA	

## MARX auf der IT-SA (13. - 15. Oktober) Halle 6, Stand 441

## Impressum

Herausgeber:  
**MARX Software Security GmbH**  
D-85104 Wackerstein  
Tel. +49(0)8403/9295-0  
Fax +49(0)8403/1500  
[sales-de@marx.com](mailto:sales-de@marx.com)  
[www.marx.com](http://www.marx.com)

All trademarks used in this newsletter are property of their respective owners.