Fallstudie: Zertifizieren von Golden Images

Strategie für intakte, sicherheitsgeprüfte System-Installationen ohne Schwachstellen

Unbemerkt können bei SW-Deployment-Prozessen Malware-Infektionen auf die Clients implementiert werden. Wie können Systemverantwortliche ihre Unternehmens-IT gegen solche Schwachstellen und Advanced Persistent Threads (APT) schützen? Den entsprechenden Fragen geht die aktuelle Fallstudie nach und schlägt eine Zertifizierung von Golden Images vor.

Die Ausgangslage

Die Gefahr, bei der Basisinstallation von Clients Schwachstellen einzubauen, ist vielfältig. «Edward Snowden» zeigt, dass APT genutzt werden. Oft werden Schwachstellen durch unsachgemäss paketierte Software im Software Deployment Prozess verursacht. Denn die Einhaltung von Terminen und Kosten werden beim Entwickeln des Softwareverteilungsprozesses stärker gewichtet als die Security. Diese steht eher beim Zyklus der Wartung und beim Patch-Management im Fokus. Ein permanenter Sicherheits-Qualitätsmanagement-Kreis existiert in diesen Entwicklungsphasen des Clientmanagements nicht. Es fehlen auch entsprechende ITIL und BSI Richtlinien.

Fallstudie: Zertifizieren von Golden Images für sicheres Client-Management

DIE ANWENDER. Software-Deployers, SW-Consultants, Desktop-Ingenieure
DIE PROBLEMATIK. Schwachstellen werden in IT-Systeme mit implementiert
DIE ANFORDERUNG. Den Standard für ein sicheres Software-Deployment setzen
DAS ZIEL. Analysierte, definierte, validierte, zertifizierte Implementierungen
DER LÖSUNGSANSATZ. Verfahren mithilfe einer Baseline effizient anwenden
DIE UMSETZUNG. Möglich nach Evaluation von Marktbedürfnis und Entwicklungspotenzial
DIE AUTOREN. Felix Hosner, Franz Steinhuber, CAS Security Incident Management (SIM); Berner Fachhochschule, Technik und Informatik Softwareschule Schweiz

Schutz vor Schwachstellen und APT

Eine Baseline als effiziente Referenzierung

Zertifikat zur Entlastung von Deployern

Die Fragestellungen und die Entwicklung der Fallstudie

Als Grundlage evaluieren wir geeignete Methoden und kombinieren sie zu Prüfverfahren. Mithilfe einer Baseline für Clients wollen wir diese koordinieren und den Zeitaufwand verkürzen, z.B. bei einem minimalen Delta an Datenveränderung. Auch kann eine Baseline ohne das Image auf aktualisierte, sicherheitsrelevante Punkte kontrolliert werden.

Diesen Fragestellungen gehen wir nach:

- Wie können wir eine Baseline erstellen?
- Welche Mittel sind umsetzungstauglich?
- Welche Tools, Vorlagen, Instrumente sind dazu nötig?
- Mit welchen Aufwänden müssen wir rechnen?
- Wo müssen wir Prioritäten setzen?
- Bestehen für ein solches Zertifikat die Voraussetzungen im Informatik-Markt?

Der Nutzen eines zertifizierten Golden Image für SW-Deployer

Das Zertifikatsverfahren erkennt Schwachstellen und Malware. Das Golden Image kann mittels Forensik-Tools bereinigt werden. Das gibt den Endkunden Sicherheit und befreit Deployers davon, zur Verantwortung gezogen zu werden.

Unser Angebot

Interessierte können sich an der Entwicklung einer allfälligen Betaversion des Zertifizieren von Golden Image beteiligen und sie zu einem marktgerechten Wertschöpfungsinstrument weiter entwickeln helfen.

Das Zertifizierverfahren von Golden Image soll diese Punkte prüfen:

- Malware mit verschiedenen Virentools
- Malware mittels Memory-Forensik
- Sniffing des Datenverkehrs
- Zertifikate
- Prozesse und ihre DLL's
- Signaturen von Files
- Dienste und Treiber
- Task Sheduler
- Autostart-Funktionen

Der Kontakt

Computer Coach GmbH
Thalgutstrasse 10 | CH–3116 Kirchdorf BE | T +41 (0)31 782 12 00 | F +41 (0)31 782 12 02
felix.hosner@computer-coach.ch