RSA 2015: Schadcode in Bilddateien – So schützen sich itWatch-Kunden schon seit Jahren!

Auf der Sicherheitskonferenz RSA Security 2015 in San Francisco stellte der Sicherheitsexperte Marcus Murray eine relativ einfache Methode vor, wie Angreifer mit verstecktem Schadcode in Bilddateien ganze Webserver übernehmen können (Details unten). Bereits auf dem Stand der itWatch, Nummer 4020 in der North Hall der RSA konnten sich die Besucher davon überzeugen, dass dieser Angriff von der itWatch Enterprise Security Suite sicher verhindert wird.

itWatch hat nämlich mit dem Modul XRayWatch der Enterprise Security Suite (itWESS) schon seit Längerem eine Lösung parat, die solch einem Angriff erfolgreich entgegenwirkt. Durch Inhaltskontrolle, Contentfilter, eine eigene Pattern-Definitions-Sprache und ein algorithmisches Patternmatching bietet das itWESS-Modul XRayWatch hier effektiven Schutz vor potentiellen Angriffen. Es ermöglicht mit seiner Pattern Prüfung die inhaltliche (semantische) und syntaktisch beliebig genaue Prüfung der Inhalte einer Datei und schließt damit ein weiteres Datenleck - Umbenennung von Dateien oder wie hier das Verstecken von Schadcode als Kommentar innerhalb der EXIF-Informationen bei einem „.JPEG“ ist damit zwecklos, da der Pattern Parser nicht nur die Nutzinhalte sondern auch die Kommentare überprüft.

Mit XRayWatch kontrollieren und protokollieren Sie exakt an den Angriffs- und Leckagepunkten, welche Daten in welchen Formaten importiert oder exportiert werden dürfen. Die firmeneigenen Informationen lassen sich überall vor dem Datenklau und gegen feindliche oder unerlaubte Dateninhalte, z.B. malicious Code, embedded Executables, schützen. Die inhaltliche Kontrolle gilt gleichermaßen für Netzwerkshares, USB-Medien oder im Firmennetz. Unternehmen überprüfen zwar an den Endpunkten ankommende und ausgehende Dateien, doch häufig nur die zulässigen Dateitypen und nicht deren Inhalte. Ausführbare Programme können jedoch in Word Dokumente eingebettet oder z.B. wie durch Marcus Murray auf der RSA 2015 bewiesen in Bilddateien versteckt sein - und damit unbemerkt Schaden anrichten.

Murray versteckte bei seinem Versuch schadhaften Code als Kommentar innerhalb der EXIF-Informationen von Bilddateien (z.B. „.jpg“, „.tiff“). Eine serverseitige Bildvorschau führte den entsprechenden Code dann aus - in diesem Fall bot der Code Zugang zur Kommandozeile des angegriffenen Servers. Über die Kommandozeile gelang es Murray danach, Stück für Stück weitere Server und Systeme des Netzwerks unter seine Kontrolle zu bekommen. Auf diese Weise gelang es ihm u. a. sich selbst Administratorenrechte im gesamten Netzwerk einer US-Bundesbehörde zu verschaffen.

In dem von Murray gezeigten Fall (> zum Artikel) schafft auch eine bessere Konfiguration des Servers Abhilfe. Die itWatch Lösung sorgt aber dafür, dass die Daten, die den Schadcode tragen gar nicht erst in das Unternehmen hereinkommen, stellen also eine sichere erste Bastion dar.

Besonderen Wert legt itWatch bei der Umsetzung der IT-Sicherheit darauf, dass IT-Sicherheit nicht als Verhinderer sondern als Business Enabler wahrgenommen wird. Dabei bedient sich itWatch eines Patentes aus dem Jahr 2000, in welchem beschrieben ist, dass die Sicherheit nicht durch das Blockieren, also das Verhindern von Funktion, entstehen sollte, sondern besser durch sichere Prozesse, die im Prinzip „alles“ erlauben, aber dafür sorgen, dass „alles“ in einer sicheren Art ausgeführt wird. Was heißt das jetzt bezogen auf den von Murray dargestellten Exploit?

Eine wichtige Rolle spielen hierbei zwei Themen:

1. Gegen den Ausbruch von Schadcode geschützte sichere Umgebungen

2. Der Anwender als Teil der technischen Sicherheitsinfrastruktur

1.) Das Modul ReCAppS (Remote Controlled Application System) ermöglicht es dem Kunden, alle sicherheitskritischen Aktionen zuerst zu erkennen und dann so zu kapseln, dass die Aktionen ausgeführt werden können, ohne dass potentielle Bedrohungen irgendeine Auswirkung haben. Der Anwender muss also jetzt nicht alle EXIF Formate, die ausführbare Elemente enthalten, strikt abweisen, sondern kann diese in einer eigens geschützten Umgebung ausführen. Wichtig ist, dass alle Aktionen des Sicherheitssystems ohne irgendeine Veränderung des Arbeitsablaufes für den Anwender voll automatisiert ausgeführt werden. Die Sicherehit ist also unsichtbar, nahtlos in die Standardabläufe integriert. Das ist die Leistung des Moduls ReCAppS.

2.) Das Modul AwareWatch der Enterprise Security Suite (itWESS) ermöglicht Security Awareness in Echtzeit und bindet den Mitarbeiter in die IT-Security des Unternehmens ein und schafft die Freiräume, die der Mitarbeiter und das Business brauchen. Mit AwareWatch tritt der Sicherheitsverantwortliche automatisiert direkt am Ort des Geschehens zum Zeitpunkt der kritischen Aktion in Dialog mit dem Anwender und zwar in Echtzeit. Der Mitarbeiter fühlt sich durch die direkte Ansprache mit Dialogen und Auswahlmöglichkeiten nicht gegängelt, sondern als aktiver Teil der Unternehmenssicherheit. In der Situation die Murray vorstellt, kann es im Sinne der Sicherheitsrichtlinie des Unternehmens sinnvoll sein, den Anwender, der dieses EXIF Dokument einbringt, vor der „Ausführung“ zu befragen, woher er dieses Dokument erhalten hat und wofür er es aus Sicht der Unternehmensprozesse benötigt. Die Antworten werden – bei Bedarf anonym – protokolliert und reichern den Life-Cycle des Objektes im Unternehmensnetzes mit sinnvollen Attributen an.