DIE ZEITSCHRIFT FÜR UNSERE KUNDEN UND GESCHÄFTSPARTNER

itsc@work

Die Lösung zählt.

magazin 2.2013 | www.itsc.de

Seite 4
iskv_21c bei der pronova BKK

Seite 8
Security Audit erfolgreich abgeschlossen

Seite 11
Jahresabschluss im itsc

Sicherheit im itsc – immer zum Greifen nah

Seite 22 itsc-Rechenzentren sind optimal geschützt

Sicherheitsüberprüfung beim itsc System-Service

Security Audit erfolgreich abgeschlossen.

Sind die itsc-Computersysteme und die darauf abgespeicherten Daten einem Hackerangriff gewachsen? Diese Frage veranlasste die Verantwortlichen des itsc bei der Firma OneConsult GmbH einen Security Audit zu bestellen, um eine Hacker-Attacke auf die vom Internet erreichbaren Systeme und Web-Applikationen zu simulieren.

oneconsult®
IT Security & Strategic Consulting

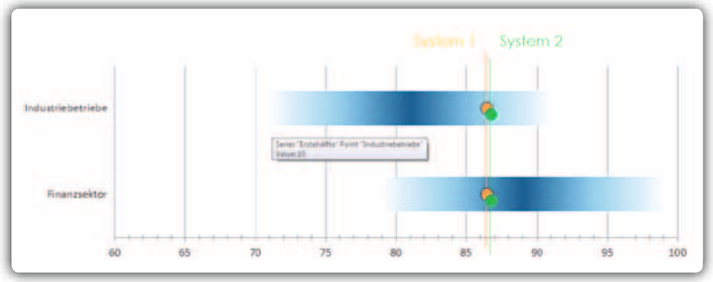
Security Audits (=technische oder konzeptionelle Sicherheitsüberprüfungen oder kurz „simulierte Hacker-Attacken") sollten laut Empfehlung zum Standard gehören und regelmäßig durchgeführt werden. Trotzdem erscheinen in den Medien gehäuft Berichte über haarsträubende Sicherheitsvorfälle. Das itsc bestellte deshalb bei der OneConsult GmbH einen Security Audit.

Vorher galt es abzuklären:

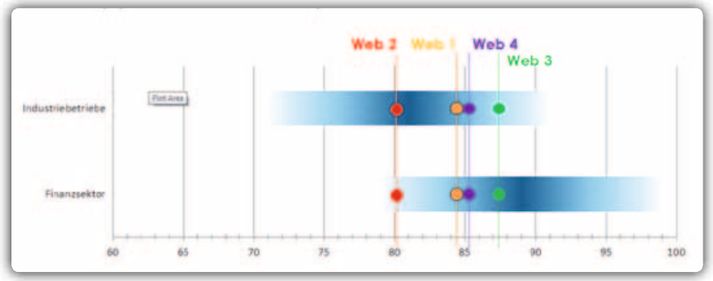
- Was kann oder sollte in einem ersten Schritt überprüft werden?
- Welches sind attraktive Angriffsziele?
- Wie viel Zeit und Geld soll investiert werden?
- Definition der Zielsysteme (Scope).

Ist der Scope definiert, entscheidet man sich für einen von drei verschiedenen Testansätzen. Beim Blackbox-Ansatz erhält der Tester keine Informationen über die Zielsysteme und deren Umgebung. Beim Greybox-Ansatz werden die nötigsten Informationen (z. B. IP-Adressen, verwendete Betriebssysteme etc.) mitgeteilt. Greybox ist der von der OneConsult empfohlene, effizienteste Ansatz mit einem optimalen Kosten-Nutzen-Verhältnis. Beim Whitebox-Ansatz liegen sämtliche Informationen offen.

Im Security Audit des itsc wurden ausgewählte, exponierte Systeme sowie Web-Applikationen nach dem Greybox-Ansatz mit folgenden Testtypen überprüft:



Penetration Test



Web Application Security Audit

Penetration Test

Gründliche, technische und unprivilegierte Sicherheitsüberprüfung mit hohem manuellen Test- und Verifikationsanteil aus der Perspektive eines Angreifers.

Im Vergleich zum Web Application Security Audit werden beim Penetration Test nur unprivilegierte Tests durchgeführt (d. h. ohne Kenntnisse von gültigen Zugangsinformationen wie User ID/Passwort etc.).

Web Application Security Audit

Gründliche, technische, unprivilegierte und privilegierte Sicherheitsüberprüfung einer Applikation und der zugehörigen Komponenten aus der Perspektive eines Angreifers.

Im Fokus: Web Applikationen und ihre zugehörigen Systeme im Front- und Backend (z. B. Internet Banking Systeme, Online Shops, SharePoint und SAP-Plattformen oder VoIP-Lösungen). Im Gegensatz zum Penetration Test werden hier auch privilegierte Tests mit Test-User ID und Passwort durchgeführt.

In beiden Disziplinen wird der Großteil der Tests manuell erbracht. Die OneConsult setzt dafür die aktuellsten Methoden und Tricks ein, welche auch „echte" Hacker/Cracker nutzen.

weiter geht's auf Seite 10 →

Testergebnisse

Um es vorweg zu nehmen: Nach der Analyse und Auswertung der Ergebnisse konnte dem itsc für die untersuchten Systeme und Applikationen ein gutes Zeugnis ausgestellt werden.

Damit Sie als Leser sich ein Bild von den untersuchten Risiken machen können, werden exemplarisch drei wichtige Sicherheitslücken aus der Top 10 Rangliste des Open Web Application Security Projects (OWASP) näher beschrieben (www.owasp.org).

Veraltete Software Versionen:
Wird eine installierte Software nicht aktuell gehalten (gepatcht), werden wichtige Sicherheitslücken nicht behoben. Somit wird die Software im Verlaufe der Zeit verwundbar und Angreifer können die Durchlässigkeit ausnutzen, um im schlimmsten Fall die Systeme zu übernehmen.

Auf den Punkt gebracht

Der RAV zeigt den Vergleich mit dem Industrie- und dem Finanzsektor. Beim itsc liegt nur eine Web-Applikation im Durchschnittsbereich des Industriesektors. Die anderen Web-Applikationen und Systeme können mit dem Durchschnitt des anspruchsvolleren Finanzsektors verglichen werden. Das itsc will die im Jahr 2012 getesteten Systeme auch 2013 wieder überprüfen lassen.

Cross Site Scripting (XSS):
Die Bezeichnung für Cross Site Scripting rührt von Befehlen von Script-Sprachen her (z. B. JavaScript). Ein Angriff erfolgt zwischen dem Aufruf zweier Seiten, z. B. beim Absenden eines Kontaktformulars (Cross-Site). Auf diese Art und Weise können beispielsweise Cookies oder auch die eindeutige Sitzungsnummer des Benutzers ausgelesen und vom Angreifer weiter verwendet werden.

„Man-in-the-Middle" (MITM) Attacke:
Dies ist ein Angriff auf den Kommunikationskanal zwischen dem Webserver und dem Anwendergerät (Client). Meistens bemerken Webserver und Client nicht, dass ein Angreifer die Kommunikation mithört. So können sensitive Daten (z. B. Passwörter etc.) erschlichen und missbraucht werden.

Methode

Die von der OneConsult angewandte OSSTMM Methode erlaubt es, aufgrund der Resultate eines Security Audits einen Benchmark, den sogenannten Risk Assessment Value (RAV), zu berechnen. Damit lassen sich die Ergebnisse des itsc mit den über 600 OSSTMM konformen Security Audits der OneConsult vergleichen.

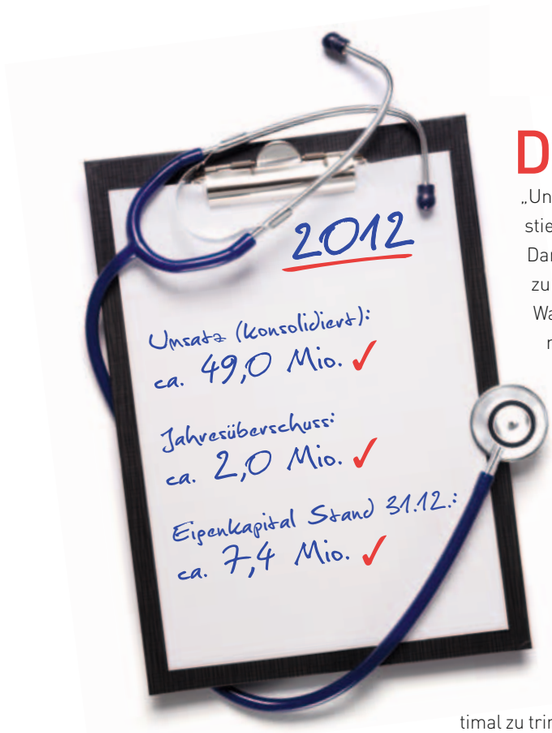
Kontakt

Tobias Ellenberger
Mediamatiker EFZ, MCTS, MCITP, OPST & OPSA; COO & Co-Partner
OneConsult GmbH
Tel. +41 79 314 25 25
tobias.ellenberger@oneconsult.com

Fit wie ein Turnschuh

Jahresabschluss im itsc.

Jedes Jahr kommt mit dem Jahresabschluss die Wahrheit auf den Tisch und es wird einem unverfälscht präsentiert, wie solide oder eben unsolide man das zurückliegende Jahr gestaltet hat. So auch beim itsc: Zwischen Januar und April untersuchten die Wirtschaftsprüfer von PricewaterhouseCoopers das Geschäftsjahr 2012 und präsentierten am Ende dem Management-Board ein erfreuliches Resultat.



Das itsc-Ergebnis kann sich wie in den Vorjahren sehen lassen. „Unser jährlicher Check-Up attestiert uns gesündeste Basiswerte. Damit haben wir beste Voraussetzungen, um steinalt zu werden. Was wir daraus machen, ist wie im richtigen Leben: Man muss am Ball bleiben und aktiv etwas für seine Gesundheit tun. Das ist uns sehr bewusst und wir haben bereits eine Menge in Richtung Zukunft angeschoben und umgesetzt", so Stefan Kreit, itsc-Geschäftsführer. „Derzeit arbeitet das itsc daran, das Unternehmen an neue Entwicklungen aus Produkt- und Marktsicht anzupassen und strategisch optimal zu trimmen. Wir tun also alles, damit auch der Check-Up im kommenden Jahr eine Routine-Untersuchung ohne negativen Befund wird."

Für eine gute Geschäftsentwicklung sind die weichen Faktoren in einem Unternehmen aber nicht minder wichtig. Denn gute Ergebnisse können nur erreicht werden, wenn man sie gemeinsam verfolgt. Hervorzuheben ist hierbei ein interner Mission & Vision Prozess, der Anfang des Jahres begonnen wurde und mit allen Mitarbeiterinnen und Mitarbeitern gemeinsam über mehrere Jahre geführt werden soll.

Kontakt

Stefan Kreit
Geschäftsführer
itsc-Gruppe
Tel. 0511 27071-105
Stefan.Kreit@itsc.de