

## IT-SOFTWARE

### Speichernetzwerk für Mac

Apple hat eine neue Version seines SAN-Filesystems für Mac OS X vorgestellt. Xsan 2 wartet mit einer komplett überarbeiteten Administrationsoberfläche auf, mit der die Einrichtung und Verwaltung eines Speichernetzwerks besonders einfach zu erledigen sein soll. Als eine der neuen Funktionen erlaubt Multi-SAN den gleichzeitigen Zugriff auf mehrere SANs von einer Arbeitsstation aus.

### Verbesserte Kundenpflege

Zum März hat Oracle den Release 15 des siebelbasierten Oracle CRM On Demand vorgestellt. Die neue Ausgabe des Online-Kundenpflegesystems soll sich insbesondere durch leistungsfähige Social-CRM-Funktionen auszeichnen. So bietet das System nun Sticky Notes und ein Message Center, über das die Anwender Kommentare in der Art von Post-It-Notizen austauschen können.

### Beziehungsmanagement

Die Schweizer Administrationssoftwarelösung Proffix Simply Business wurde um ein CRM-Modul erweitert. Dieses soll Kunden beim Beziehungsmanagement unterstützen und bei der langfristigen Kundenpflege helfen. Proffix CRM kann mit Infofenstern aufwarten, die einen raschen Überblick über die Pendenzen pro Kunde bieten und die jeder Mitarbeiter für sich frei definieren kann.

### Adobe Rechteverwaltung

Adobe hat den Flash Media Rights Management Server auf den Markt gebracht, eine neue Serverlösung für den Schutz von Flash-Inhalten wie Videos im Adobe Flash Player, im Adobe Media Player und in Adobe AIR. Der Rechteverwaltungs-Server soll präzise Kontrollmöglichkeiten darüber bieten, wie und für wie lange bestimmte Inhalte genutzt werden können. Zudem kann die Weiterverwendung von Inhalten geregelt werden.

### Angepasstes Reporting

Combit hat sein Reporting-Werkzeug List & Label 13 im Hinblick auf den Release von Visual Studio 2008 überarbeitet. So steht per sofort eine angepasste VS.Net Assembly bereit. Damit soll sich die Lösung nahtlos in Projekte integrieren lassen, welche mit Microsofts allerneuester Entwicklungsumgebung erstellt wurden. Einige Beispiele für die aktualisierte .Net-Komponente werden mitgeliefert.

# Von Hackern und ihren Nachahmern

Aufgrund steigender Internetkriminalität und der Zunahme von gesetzlichen Vorgaben erleben technische Audits einen Boom. Allerdings ist es schwierig, kompetente Tester zu finden und ihnen die richtigen Fragen zu stellen.

Technische Audits haben zum Ziel, Sicherheitslücken aufzudecken, bevor sie von Unberechtigten ausgenutzt werden können. Mögliche Untersuchungsobjekte sind dabei Systeme im Local Area Network, kabellose Netzwerke, Applikationen und Systeme in der demilitarisierten Zone (DMZ). Eine DMZ ist ein System, welches zumindest teilweise vom Internet her erreichbar ist, so zum Beispiel Firewall, Web-, Mail-, und DNS-Server sowie Netzwerkkomponenten. Technische Audits lassen sich hinsichtlich des Untersuchungsobjekts, der Testtiefe und -breite und des Automatisierungsgrads grob kategorisieren. Je nach Testtiefe bzw. -breite werden Sicherheitslücken mittels eher oberflächlicher Scans gesucht, oder Lücken auch konkret ausgenutzt. Genauso kann nur die Systemkonfiguration oder ebenfalls der Applikationsquellcode geprüft werden. Eine weitere Kategorisierung betrifft den Automatisierungsgrad. Damit wird beschrieben, wie viel Expertenwissen für ein Tool wie beispielsweise einen Security Scanner eingebracht werden muss.

### Security Scan oder Penetration Test?

Ein Security Scan ist eine hochautomatisierte, netzwerkbasierte Sicherheitsüberprüfung, bei welcher von Tools entdeckte Sicherheitslücken teilweise manuell verifiziert werden. Im Gegensatz dazu ist der Penetration Test eine zwar ebenfalls netzwerkbasierte, aber intensivere Sicherheitsüberprüfung. Dabei werden Sicherheitslücken manuell ausgenutzt. Automatisierte Tools kommen hier nur zum Einsatz, wenn sie den Projektlauf beschleunigen können, ohne dass die Qualität darunter leidet. Von den Testern wird also viel Expertenwissen abverlangt. Das Problem dabei ist, dass niemand auf alle relevanten Gebiete der ICT spezialisiert sein kann, niemand kann sich in Betriebssystemen, Firmwares, Datenbanken, Exploit-Programmierung und Programmiersprachen gleichzeitig auskennen. Somit kommt bei Penetration Tests meist ein Team von Experten verschiedener Spezialisierungsrichtungen zum Einsatz. Manche Anbieter verfügen aber gar nicht über

mehrere Tester und versuchen dieses Manko mit Tools wettzumachen. Allerdings geht diese Rechnung für den Anbieter nur auf, wenn der Kunde nicht über profundes Fachwissen der Materie verfügt. Andernfalls verkommen die vor Ort zu leistenden Arbeiten wie Kickoff-Meeting, Tests und Projektschlusspräsentation zum Spiessrutenlauf für das damit betraute Personal des Anbieters. In solchen Fällen wäre es für alle Beteiligten besser, die Dienstleistung würde dem Kunden ehrlich als simpler Security Scan verkauft – anstatt als vermeintlicher Penetration Test. Um die Vergleichbarkeit der Testresultate zu gewährleisten, fordern manche Kunden auch, dass sich die Anbieter an erkannte Methoden wie beispielsweise dem «Open Source Security Testing Methodology Manual» (OSSTMM) halten.

### Kundenanforderungen

KMU beauftragen oft ihre angestammten Systemintegratoren mit der Durchführung von technischen Audits – wobei es sich bei der angebotenen Dienstleistung meist um einen Test der Qualitätsgüte eines Security Scans handelt. Unternehmen in streng regulierten Branchen wie beispielsweise der Finanz- und Pharmaindustrie legen Wert auf Gewaltentrennung und Produktunabhängigkeit. Denn nur so laufen sie nicht Gefahr, dass der Anbieter das Audit-Projekt als Wegbereiter für weitere Verkaufsaktivitäten nutzt. Ausserdem wird bei Systemintegratoren oft die fehlende Fokussierung auf technische Audits bemängelt. Meistens haben sie nämlich nur ein bis zwei Mitarbeiter, welche sich bestenfalls sporadisch mit Sicherheitsüberprüfungen beschäftigen. Auf technische Audits spezialisierte Nischenanbieter haben deshalb gute Karten, sofern sie es schaffen, einen genügend grossen Personalbestand an Security Testern aufzubauen und dank ausreichender Projektauslastung zu halten.

### Schwierige Personalrekrutierung

Bei komplexen technischen Audits wird sozusagen am offenen Herzen der ICT-Infrastruktur operiert. Deshalb sind der gute Ruf des Anbieters, der tadellose Leumund und das Ex-

pertenwissen der Security Tester entscheidend. Die Problematik beim Rekrutieren von Security Testern, liegt darin, dass spezifische «Hackerkenntnisse» nicht in der Informatikerlehre oder an Hochschulen vermittelt werden. Die meisten Security Tester sind also über ihr Hobby zum Beruf gekommen. Ihre Ausbildung basiert somit auf Erfahrung und einer guten persönlichen Vernetzung zu anderen Security Testern. Falls die Kandidaten in der Vergangenheit mit dem Gesetz in Konflikt geraten sind, haben sie sich damit für einen seriösen Einsatz disqualifiziert.

### Risiken, Aufwand und Kosten

Technische Audits lassen sich teilweise kaum von echten Hackerattacken unterscheiden. Der Auftraggeber muss deshalb einen Haftungsausschluss unterschreiben. In diesem bestätigt er, darüber in Kenntnis gesetzt worden zu sein, dass es bei technischen Audits zu negativen Systembeeinträchtigungen kommen kann. Ausserdem ist wie bei allen Projekten die Management Attention und die klare Definition der Projektziele, Rahmenbedingungen, Ansprechpartner inklusive Eskalationspfade und Zeitplanung für den Projekterfolg essentiell.

Technische Audits sind ein interessantes Betätigungsfeld. Wer sich jedoch als Anbieter von anspruchsvollen technischen Audits etablieren möchte, benötigt hervorragende Security Tester und eine klar erkennbare Fokussierung. Die branchenüblichen Tagessätze für derartige Leistungen liegen zwischen 1600 und 2500 Franken pro Arbeitstag.

### DER AUTOR

Christoph Baumgartner (39) ist CEO und Inhaber der Oneconsult GmbH. Oneconsult ist ein international tätiges Schweizer



IT-Security-Consulting-Unternehmen mit Schwerpunkt technische Audits. Oneconsult hat Büros in der Schweiz, Deutschland, Frankreich und Österreich.  
www.oneconsult.com