WIR SPRECHEN MIT CHRISTOPH BAUMGARTNER

Christoph Baumgartner ist Geschäftsführer der OneConsult GmbH. Das Unternehmen bietet Beratungsleistungen in den Bereichen IT Security und Strategie an.

Ihre Firme existiert nun seit etwa sechs Jahren. Können Sie uns einen Abriss der Entwicklung Ihrer Firma OneConsult, geben? Seit wann genau existiert Ihr Unternehmen und wie hat es sich seither entwickelt? Wie viele Mitarbeiter und Kunden können Sie mittlerweile verzeichnen?
Ich habe die Firma im Juni 2003 zusammen mit meiner Frau gegründet. Seither hat sich viel getan: Eröffnung der Vertretung Deutschland in Neu-Ulm im Mai 2006, Eröffnung der Filiale Bern im Juni 2006, Eröffnung der Niederlassung Österreich in Wien im Mai 2007, Gründung der Tochtergesellschaft OneConsult Deutschland GmbH in Neu-Ulm im Juni 2007 und die Eröffnung der Niederlassung Frankreich in Lyon im März 2008. Von unseren 18, grösstenteils vollzeitbeschäftigten Mitarbeitern sind 11 Security Tester. Unser Kundenstamm umfasst weit über 100 Kunden in vielen Europäischen Ländern. Die meisten Kunden bleiben uns nach dem ersten Auftrag treu.

Hatten Sie bereits vor der Gründung von OneConsult Erfahrung im Bereich der Computersicherheit? War es schwer im deutschsprachigen Raum Fuß zu fassen?
Ich bin seit 1996 als IT Security Consultant tätig. Dabei konnte ich bereits früh Führungserfahrung bei verschiedenen namhaften System- und Security-Integratoren sammeln. Bei meinem letzten Arbeitgeber hatte ich das bis dahin dort inexistente IT Security Consulting aufgebaut.

Produktunabhängigkeit gesetzt. Aufgrund dieses Kredos findet sich meines Wissens nach selbst nach über 250 technischen Security Audits kein einziger unzufriedener Kunde. Dank der daraus resultierenden Mund-zu-Mund-Propaganda und unserem fähigen und sehr motivierten Team gelang es uns aus der Schweiz heraus immer mehr Kunden ausserhalb der Schweiz zu gewinnen. Dies bildete eine solide Basis für die Gründung unserer deutschen Tochter, welche seither einen festen Platz in der IT Security Consulting Branche hat.

Sie bieten viele verschiedene Dienstleistungen an, wie etwa Security Scans, Penetration Tests, Forensische Analysen, Schulungen und noch einige mehr. Welche davon werden von ihren Kunden am häufigsten beantragt? Obwohl vermutlich nicht verallgemeinerbar – wie lange dauert durchschnittlich ein Auftrag von Planung, Durchführung bis hin zum Reporting?
Historisch bedingt nehmen uns die meisten Kunden primär als Anbieter anspruchsvoller technischer Security Audits wahr. Aus diesem Grund werden hauptsächlich Penetration Tests und Application Security Audits bestellt. Die Security Scans weisen dagegen einen hohen Automatisierungsgrad auf. Deshalb kommen Security Scans hauptsächlich als Ergänzung zum Zug, wenn beispielsweise eine grosse Anzahl Systeme bei kleinem Budget getestet werden soll. Immer öfter bieten uns Kunden nach einem Security Incident wie einer erfolgreichen Hacker- oder Malwareattacke auf, damit wir die Ursache analysieren und bei der Umsetzung von Gegenmassnahmen behilflich sind. Je länger je mehr führen wir auch konzeptionelle Security Audits nach ISO/IEC 2700x oder BSI Standard-100-x und gezielte Schulungen und Coaching durch.

Security Audits dauern zwischen wenigen Tagen bis zu mehreren Monaten. Dies ist abhängig von der Komplexität des Untersuchungsobjekts und dem Schutzbedarf des Kunden.

Sie verzeichnen zu ihren Kunden Unternehmen aus den Bereichen Bankwesen, Militär, Gesundheitswesen, Industrie etc. Obwohl sie verschiedene Dienstleistungen anbieten, können Sie uns mitteilen, ob für Security Consultants eine gewisse Routine vorliegt, da viele Aufgaben nach demselben Schema ablaufen (beispielsweise Auditierung nach OSSTMM)?
Weil wir unsere Penetration Tests üblicherweise OSSTMM-konform durchführen, haben unsere Kunden die Garantie, dass das Vorgehen standardisiert ist und somit die Resultate vergleichbar sind. Die Durchführung zugehöriger Basistests gehört zwangsläufig zu den weniger herausfordernden Routineaufgaben

jedes Security Testers. In der Regel bleibt in den meisten Projekten dennoch genügend kreativer Spielraum bei den tiefer gehenden Zusatztasks (z.B. für Reverse Engineering und Exploiting). Ausserdem sind wir so organisiert, dass unsere Mitarbeiter Standort-übergreifend den Know-how-Austausch pflegen, regelmässig interne Schulungen durch eigene Mitarbeiter anbieten und spezifische Events besuchen um sich mit Berufskollegen auszutauschen.

Was können Sie jungen Leuten empfehlen, die sich für Computersicherheit interessieren und eine Karriere als IT Security Consultant anstreben?

Besonders wichtig sind fünf Dinge: Ausbildung, Wissensdurst, Engagement, seriöses Auftreten und tadelloser Leumund. Insbesondere der letzte Punkt wird oft unterbewertet, aber keine seriöse Security Consulting Firma würde Leute einstellen, welche in ihrer Vergangenheit als Black Hats tätig waren. Denn wer lässt sein Haus von einem ortsbekannten Einbrecher bewachen?

Inwiefern engagieren Sie sich selbst auf technischer Ebene bei ihren Dienstleistungen? Ist aufgrund der umfangreichen Arbeit das Privatleben eingeschränkt?

In den ersten Jahren von OneConsult habe ich aktiv mit getestet. Doch seither überlasse ich das Testen unseren Spezialisten. Ich bin aber noch im Bereich Qualitätssicherung (das OSSTMM fordert das 4-Augen-Prinzip) und im konzeptionellen Security Consulting tätig. Da meine durchschnittliche Wochenarbeitszeit zwischen 50 und 70 Stunden beträgt ist mein Privatleben zwangsläufig davon tangiert. Aber als Unternehmer weiss man, auf was man sich da einlässt.

Was sind Ihre Ansichten zu Zertifikaten im Sicherheitsbereich, wie etwa CISSP, CEH, CPTS, OPST etc.?

Die von Ihnen genannten Zertifikate haben alle ihre Berechtigung. Das Zertifikat belegt zumindest, dass die Person zum Prüfungszeitpunkt den Prüfungsstoff korrekt wiedergeben konnte. Als Security Consultant sind Zertifizierungen vor allem in der Akquisitionsphase hilfreich. Da OneConsult generell OSSTMM-konforme Penetration Tests durchführt, können wir mit den OSSTMM-bezogenen Zertifizierungen unserer Mitarbeiter belegen, dass OSSTMM für OneConsult mehr als ein Marketingschlagwort ist.

Worin besteht Ihrer Meinung nach der Vorteil von OSSTMM gegenüber anderen Audit-Richtlinien wie etwa dem GSHB vom BSI und anderen?

Das Open Source Security Testing Methodology Manual (OSSTMM) ist die am weitesten verbreitete Methode für die Planung, Durchführung und Dokumentation von technischen Security Audits. Im Gegensatz dazu wird im GSHB und in ISO/IEC 2700x nicht im Detail auf die Durchführung von Penetrationstests eingegangen. Das OSSTMM versteht sich somit als Ergänzung und nicht als Konkurrenz zu anderen Standards und hat sich auch ausserhalb des deutschsprachigen Raums etabliert.

Wir bedanken uns für das Gespräch!